Fernando Machado
CISO, Cybersec Investments

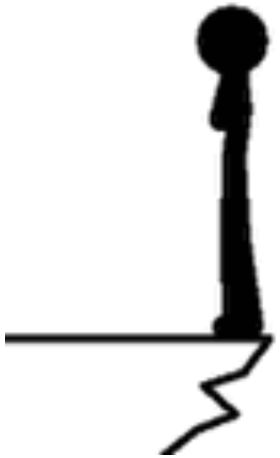
- ***<u>Cybersecurity Consulting</u>***:
  - *10+ years DoD cybersecurity experience*
  - *NIST 800-171: Controlled Unclassified Information (CUI)*
  - *Army, Navy, Air Force customer experience*
- ***<u>Certified</u>***:
  - *Certified CMMC Assessor (CCA)*
  - *Certified CMMC Professional (CCP)*
  - *Authorized CMMC 3rd Party Assessment Organization (C3PAO)*
- ***<u>Awards</u>***:
  - *President's Volunteer Service Award*

1900 S Harbor City Blvd. Suite 328
Melbourne, Florida 32901

info@cybersecinvestments.com
1-800-960-8802

Follow us on LinkedIn:

CUI-CON



CMMC PITFALLS

DFARS 252.204-7012

DFARS 252.204-7019

CYBERSECURITY MATURITY MODEL

CERTIFICATION

DFARS 252.204-7021

DFARS 252.204-7020

NIST SPECIAL PUBLICATION

SP 800-171

171

REVISION 2

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

The DFARS Series

DFARS 252.204-7012

DFARS 252.204-7019

CYBERSECURITY MATURITY MODEL CERTIFICATION

DFARS 252.204-7021

DFARS 252.204-7020

What is the Defense Federal Acquisition Regulation Supplement (DFARS)?

- *"The Defense Federal Acquisition Regulation Supplement (DFARS) to the Federal Acquisition Regulation (FAR) is administered by the Department of Defense (DoD). The DFARS implements and supplements the FAR. The DFARS contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on the public."*

What is the Defense Federal Acquisition Regulation Supplement (DFARS)?

- *"The Defense Federal Acquisition Regulation Supplement (DFARS) to the Federal Acquisition Regulation (FAR) is administered by the Department of Defense (DoD). The DFARS implements and supplements the FAR. The DFARS contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on the public."*

What is the Defense Federal Acquisition Regulation Supplement (DFARS)?

- *"The Defense Federal Acquisition Regulation Supplement (DFARS) to the Federal Acquisition Regulation (FAR) is administered by the Department of Defense (DoD). The DFARS implements and supplements the FAR. The DFARS contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on the public."*

What is the Defense Federal Acquisition Regulation Supplement (DFARS)?

- *"The Defense Federal Acquisition Regulation Supplement (DFARS) to the Federal Acquisition Regulation (FAR) is administered by the Department of Defense (DoD). The DFARS implements and supplements the FAR. The DFARS contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on the public."*

DFARS 252.204-7012: Safeguarding covered defense information and cyber incident reporting

DFARS 252.204-7012: Safeguarding covered defense information and cyber incident reporting

- *“Covered contractor information system” means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.*

DFARS 252.204-7012: Safeguarding covered defense information and cyber incident reporting

- *"Covered contractor information system" means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.*

DFARS 252.204-7012: Safeguarding covered defense information and cyber incident reporting

- *"Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies*

DFARS 252.204-7012: Safeguarding covered defense information and cyber incident reporting

- *"Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies*

DFARS 252.204-7012: Safeguarding covered defense information and cyber incident reporting

- *“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.*

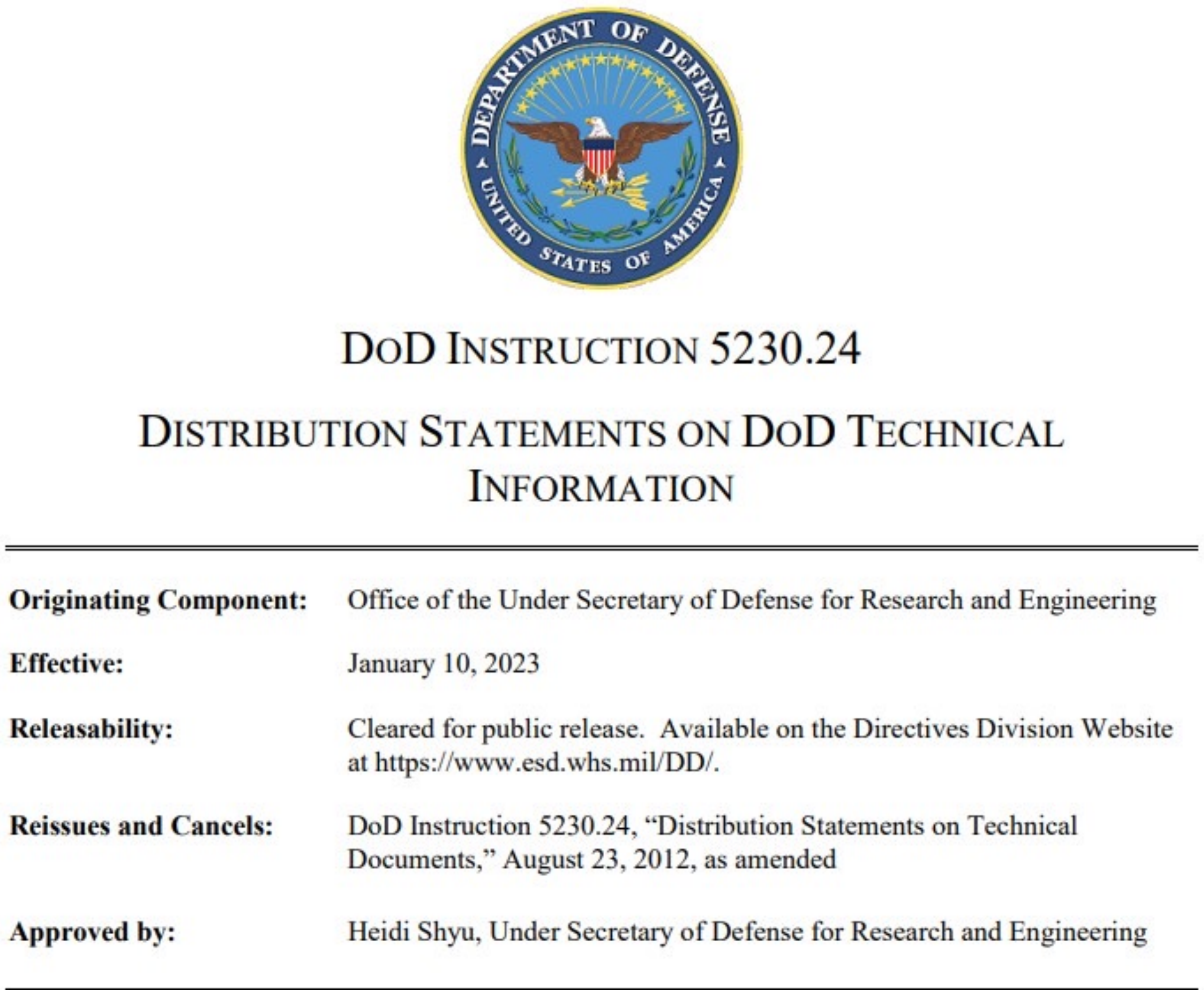
DFARS 252.204-7012: Safeguarding covered defense information and cyber incident reporting

- *“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.*

DFARS 252.204-7012: Safeguarding covered defense information and cyber incident reporting

- *"Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.*

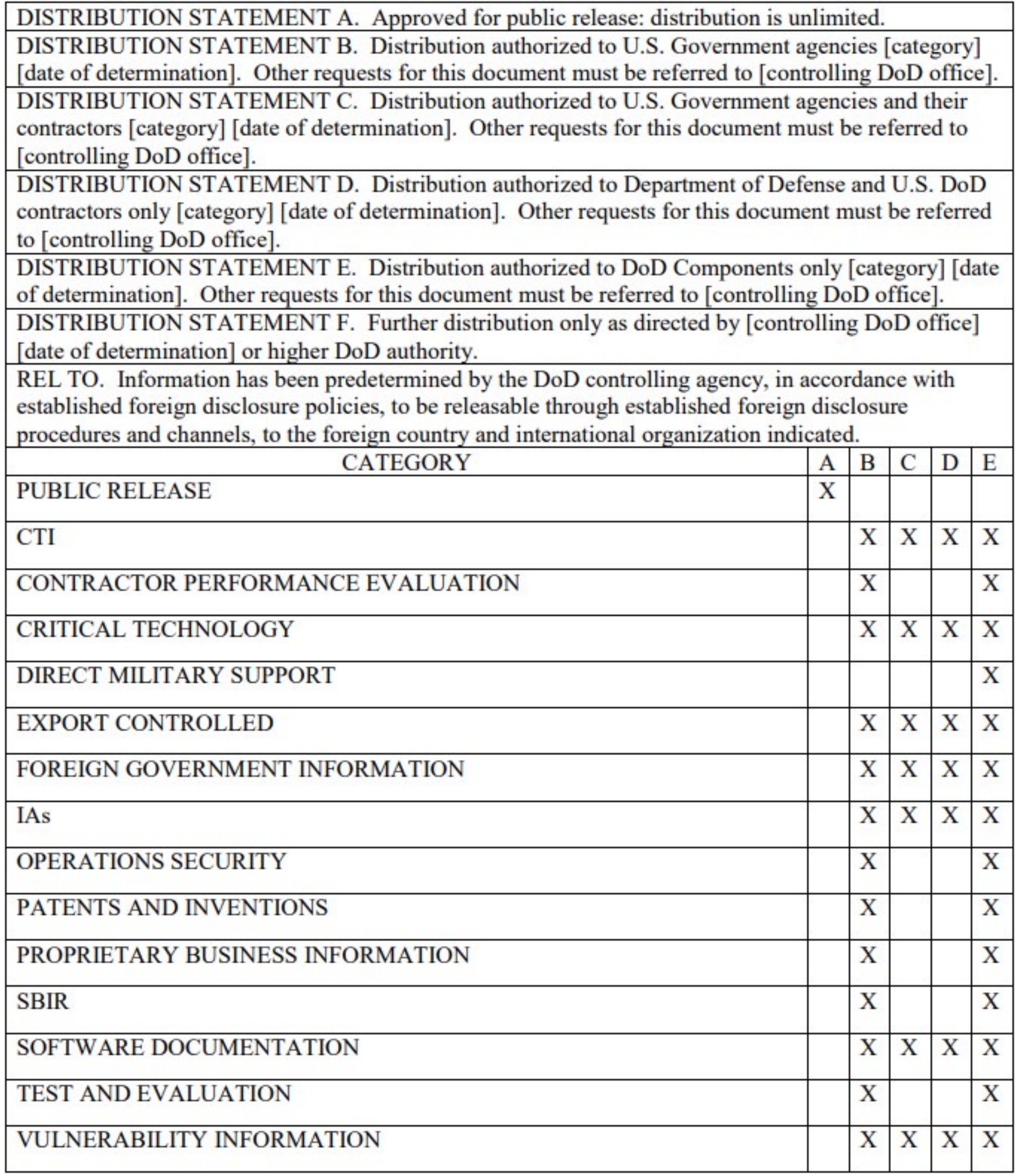
DoD Instruction 5230.24



DoD Instruction 5230.24

Distribution Statements on DoD Technical Information

Originating Component:	Office of the Under Secretary of Defense for Research and Engineering
Effective:	January 10, 2023
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23, 2012, as amended
Approved by:	Heidi Shyu, Under Secretary of Defense for Research and Engineering



DISTRIBUTION STATEMENT A. Approved for public release: distribution is unlimited.

DISTRIBUTION STATEMENT B. Distribution authorized to U.S. Government agencies [category] [date of determination]. Other requests for this document must be referred to [controlling DoD office].

DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government agencies and their contractors [category] [date of determination]. Other requests for this document must be referred to [controlling DoD office].

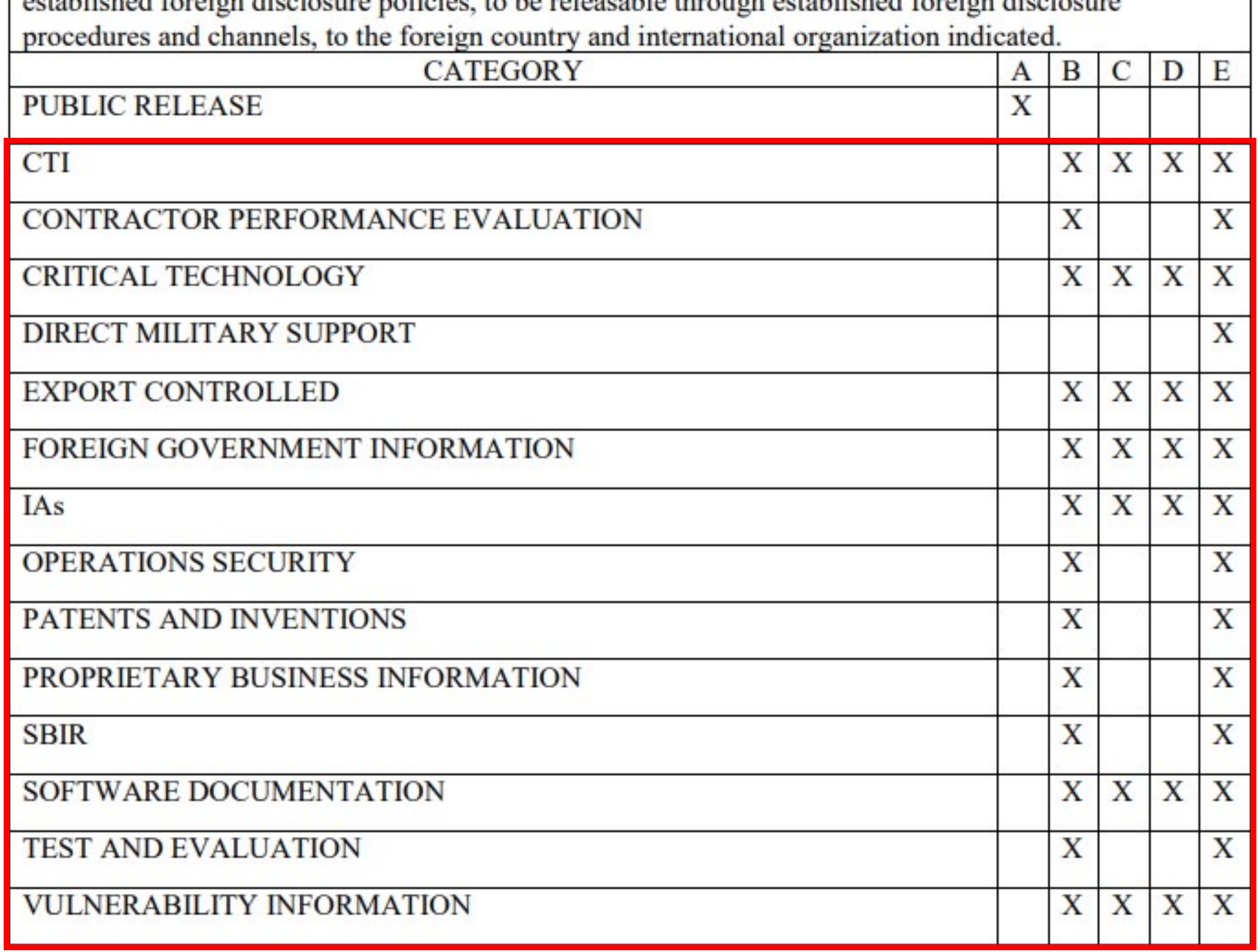
DISTRIBUTION STATEMENT D. Distribution authorized to Department of Defense and U.S. DoD contractors only [category] [date of determination]. Other requests for this document must be referred to [controlling DoD office].

DISTRIBUTION STATEMENT E. Distribution authorized to DoD Components only [category] [date of determination]. Other requests for this document must be referred to [controlling DoD office].

DISTRIBUTION STATEMENT F. Further distribution only as directed by [controlling DoD office] [date of determination] or higher DoD authority.

REL TO. Information has been predetermined by the DoD controlling agency, in accordance with established foreign disclosure policies, to be releasable through established foreign disclosure procedures and channels, to the foreign country and international organization indicated.

CATEGORY	A	B	C	D	E
PUBLIC RELEASE	X				
CTI		X	X	X	X
CONTRACTOR PERFORMANCE EVALUATION		X			X
CRITICAL TECHNOLOGY		X	X	X	X
DIRECT MILITARY SUPPORT					X
EXPORT CONTROLLED		X	X	X	X
FOREIGN GOVERNMENT INFORMATION		X	X	X	X
IAs		X	X	X	X
OPERATIONS SECURITY		X			X
PATENTS AND INVENTIONS		X			X
PROPRIETARY BUSINESS INFORMATION		X			X
SBIR		X			X
SOFTWARE DOCUMENTATION		X	X	X	X
TEST AND EVALUATION		X			X
VULNERABILITY INFORMATION		X	X	X	X



established foreign disclosure policies, to be releasable through established foreign disclosure procedures and channels, to the foreign country and international organization indicated.

CATEGORY	A	B	C	D	E
PUBLIC RELEASE	X				
CTI		X	X	X	X
CONTRACTOR PERFORMANCE EVALUATION		X			X
CRITICAL TECHNOLOGY		X	X	X	X
DIRECT MILITARY SUPPORT					X
EXPORT CONTROLLED		X	X	X	X
FOREIGN GOVERNMENT INFORMATION		X	X	X	X
IAs		X	X	X	X
OPERATIONS SECURITY		X			X
PATENTS AND INVENTIONS		X			X
PROPRIETARY BUSINESS INFORMATION		X			X
SBIR		X			X
SOFTWARE DOCUMENTATION		X	X	X	X
TEST AND EVALUATION		X			X
VULNERABILITY INFORMATION		X	X	X	X

DoD Procurement Toolbox

- *Q27: If a Contract document (i.e., DD Form 1423-1) mandates the use of a Distribution Statement (B-F) on a contractor generated document for submission to the government but does not use the term CUI, should the contractor understand the document to be CUI and protect/control accordingly? Is it correct to say that any document with a Distribution Statement B-F is CUI?*
- *A27: CUI, as defined by 32 CFR 2002, CUI, is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. Because Distribution Statements B-F as set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents, are in fact 'dissemination controls', this information is – by definition – CUI.*

DoD Procurement Toolbox

- *Q27: If a Contract document (i.e., DD Form 1423-1) mandates the use of a Distribution Statement (B-F) on a contractor generated document for submission to the government but does not use the term CUI, should the contractor understand the document to be CUI and protect/control accordingly? Is it correct to say that any document with a Distribution Statement B-F is CUI?*
- *A27: CUI, as defined by 32 CFR 2002, CUI, is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. Because Distribution Statements B-F as set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents, are in fact 'dissemination controls', this information is – by definition – CUI.*

DoD Procurement Toolbox

- *Q27: If a Contract document (i.e., DD Form 1423-1) mandates the use of a Distribution Statement (B-F) on a contractor generated document for submission to the government but does not use the term CUI, should the contractor understand the document to be CUI and protect/control accordingly? Is it correct to say that any document with a Distribution Statement B-F is CUI?*
- *A27: CUI, as defined by 32 CFR 2002, CUI, is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. Because Distribution Statements B-F as set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents, are in fact 'dissemination controls', this information is – by definition – CUI.*

DFARS 252.204-7012: Safeguarding covered defense information and cyber incident reporting

- *“Rapidly report” means within 72 hours of discovery of any cyber incident.*

DFARS 252.204-7012(b)(2)(i)

- *Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.*

DFARS 252.204-7012(b)(2)(i)

- *Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.*

DFARS 252.204-7012(b)(2)(i)

- *Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.*

DFARS 252.204-7012(b)(2)(ii)(A)

- *The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.*

DFARS 252.204-7012(b)(2)(ii)(A)

- *The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.*

DFARS 252.204-7012(b)(2)(ii)(D)

- *If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.*

DFARS 252.204-7012(b)(2)(ii)(D)

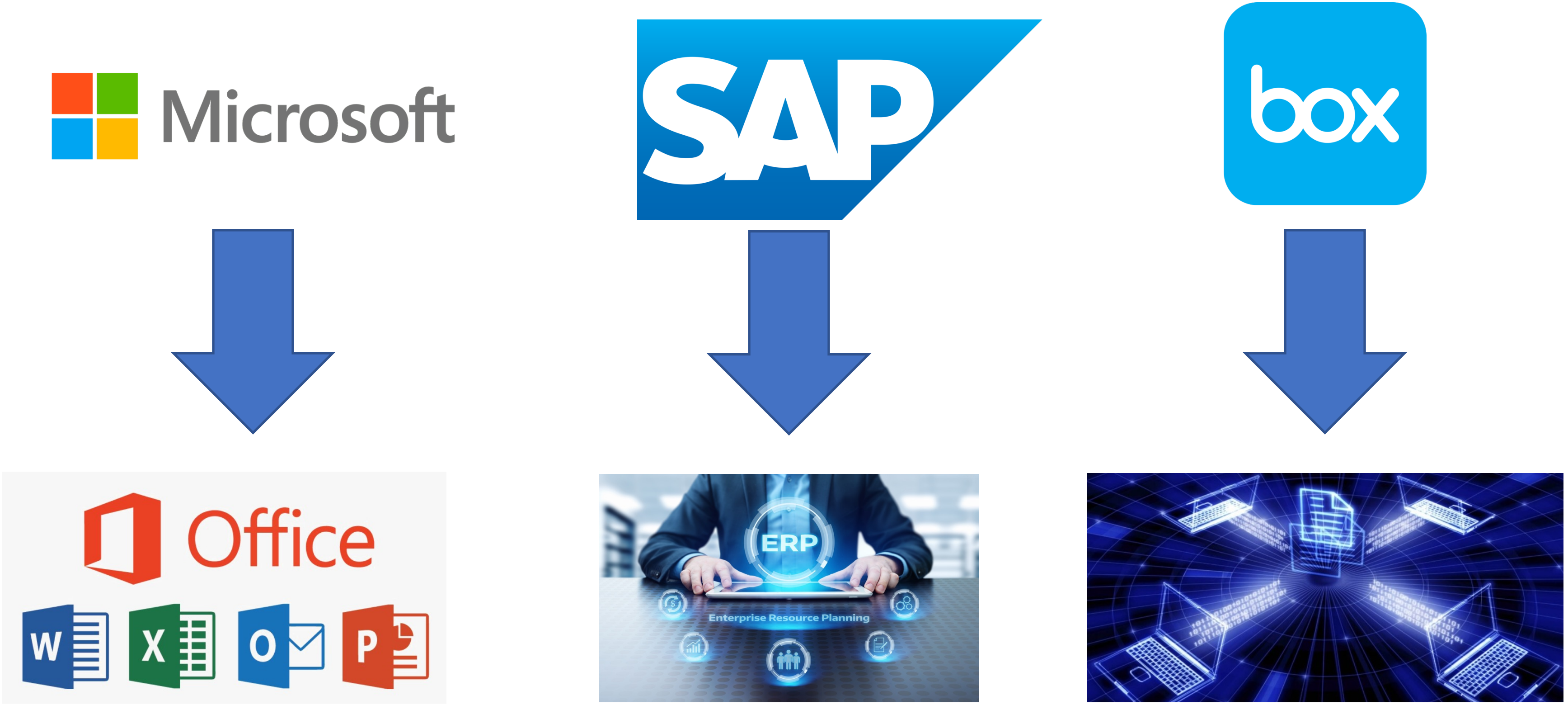
- *If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.*

DFARS 252.204-7012(b)(2)(ii)(D)

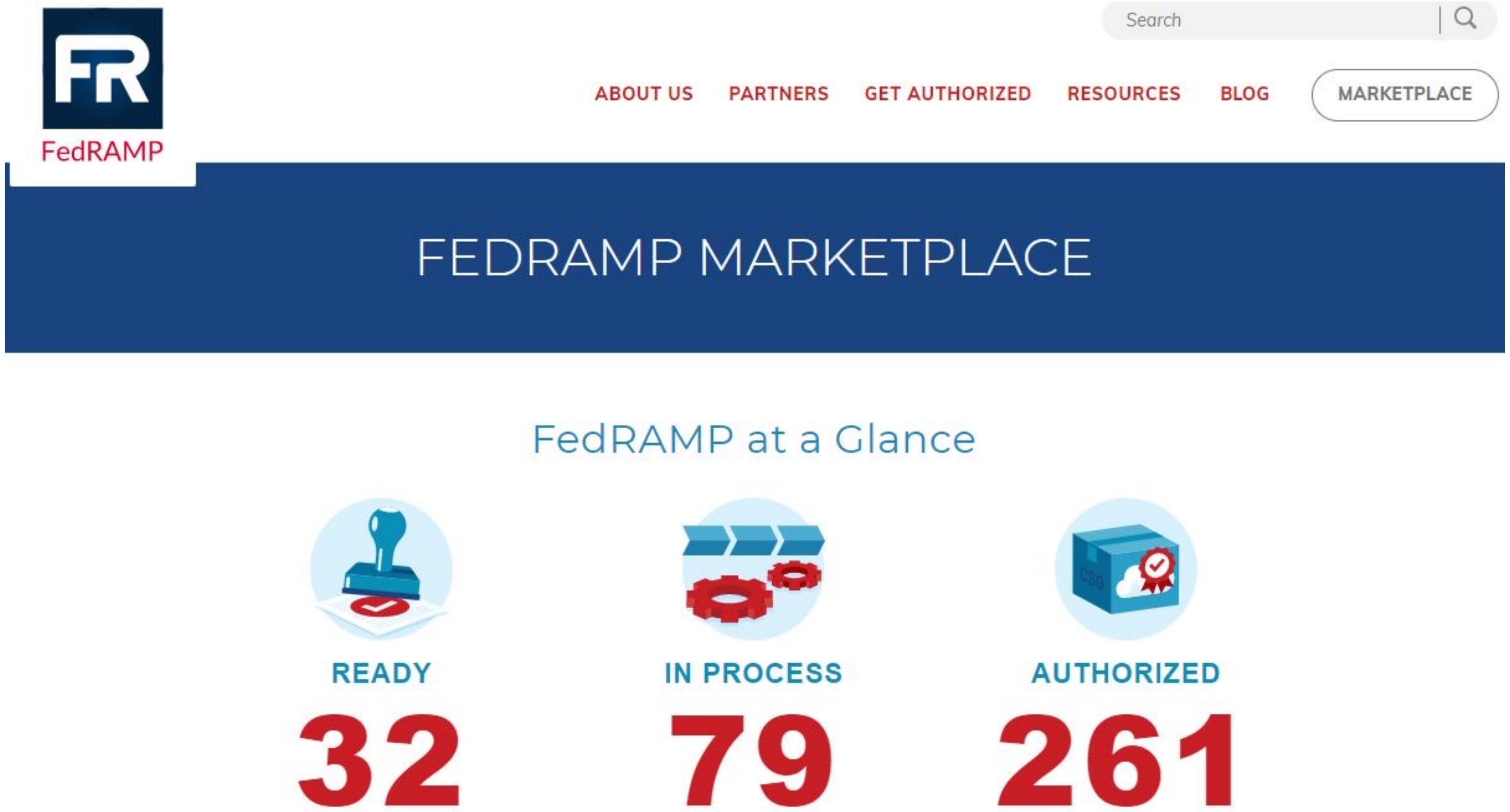
- *If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.*

DFARS 252.204-7012(b)(2)(ii)(D)

- Examples of cloud service providers:



FedRAMP Marketplace



FedRAMP

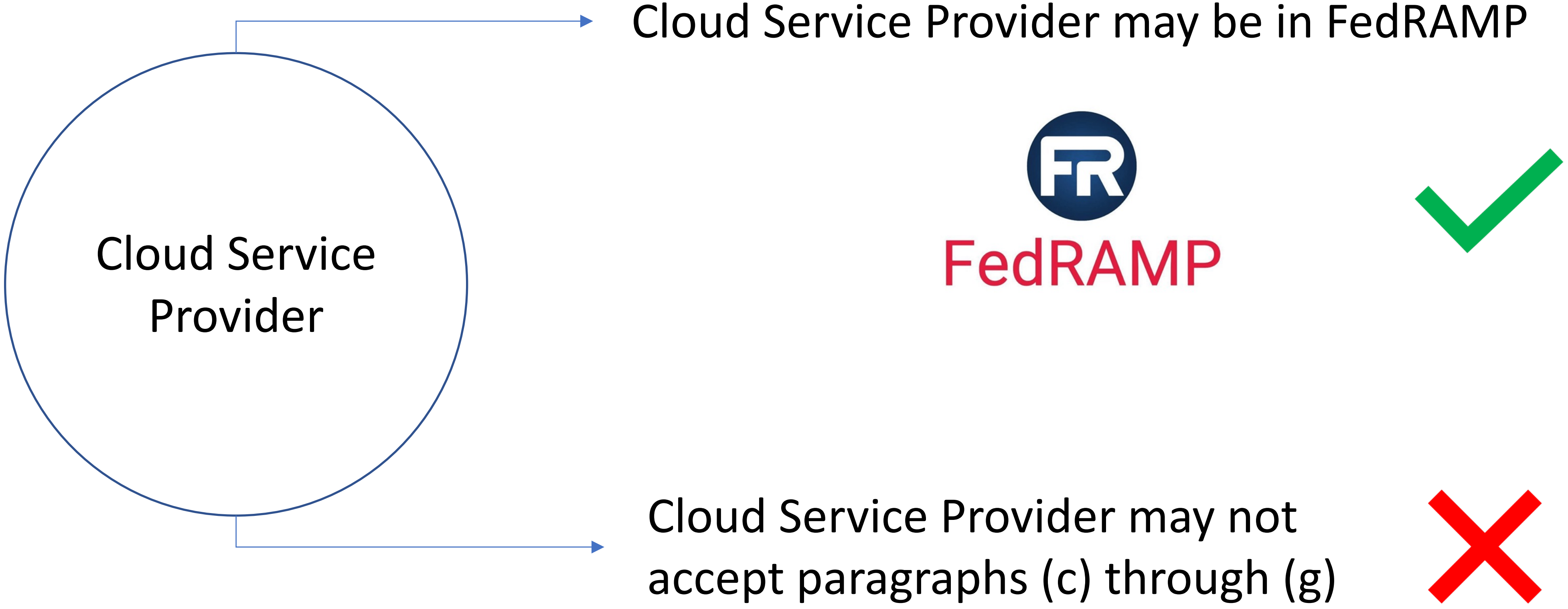
Search

FEDRAMP MARKETPLACE

FedRAMP at a Glance

READY	IN PROCESS	AUTHORIZED
32	79	261

DFARS 252.204-7012 Requirements



Cloud Service Provider

Cloud Service Provider may be in FedRAMP

FedRAMP ✓

Cloud Service Provider may not accept paragraphs (c) through (g) ✗

DFARS 252.204-7012 Requirements

	Microsoft 365 “Commercial”			
Customer Eligibility	**Any customer**			
Datacenter Locations	**US & OCONUS**			
FedRAMP [1]	**High**			
DFARS 252.204-7012	**No**			
FCI + CMMC L1	**Yes**			
CUI / CDI + CMMC L2-3	**No**			
ITAR / EAR	**No**			
DoD CC SRG Level [2]	**N/A**			
NIST SP 800-53 / 171 [3]	**Yes**			
CJIS Agreement	**No**			
NERC / FERC	**No**			
Customer Support	Worldwide / Commercial Personnel			
Directory / Network	Azure “Commercial”			

[1] *Equivalency*, Supports accreditation at noted impact level

[2] *Equivalency*, PA issued for DoD only

[3] Organizational Defined Values (ODV's) will vary

^ CUI Specified (*e.g., ITAR, Nuclear, etc.*) not suitable REQS US Sovereignty

DFARS 252.204-7012 Requirements

	Microsoft 365 “Commercial”			
Customer Eligibility	**Any customer**			
Datacenter Locations	**US & OCONUS**			
FedRAMP [1]	**High**			
DFARS 252.204-7012	**No**			
FCI + CMMC L1	**Yes**			
CUI / CDI + CMMC L2-3	**No**			
ITAR / EAR	**No**			
DoD CC SRG Level [2]	**N/A**			
NIST SP 800-53 / 171 [3]	**Yes**			
CJIS Agreement	**No**			
NERC / FERC	**No**			
Customer Support	Worldwide / Commercial Personnel			
Directory / Network	Azure “Commercial”			

[1] *Equivalency*, Supports accreditation at noted impact level

[2] *Equivalency*, PA issued for DoD only

[3] Organizational Defined Values (ODV’s) will vary

^ CUI Specified (*e.g., ITAR, Nuclear, etc.*) not suitable REQS US Sovereignty

DFARS 252.204-7012(c): Cyber Incident Reporting Requirement

- *Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.*

DFARS 252.204-7012(c): Cyber Incident Reporting Requirement

- *Medium assurance certificate requirement. In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.*

DFARS 252.204-7012(c): Cyber Incident Reporting Requirement

- *Medium assurance certificate requirement. In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.*

widepoint

IdenTrust™
part of HID Global

DFARS 252.204-7012(d): Malicious Software

- *Malicious software. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.*

DFARS 252.204-7012(d): Malicious Software

- *Malicious software. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.*

DFARS 252.204-7012(d): Malicious Software

- *Malicious software. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.*

DFARS 252.204-7012(e): Media Preservation and Protection

- *Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.*

DFARS 252.204-7012(e): Media Preservation and Protection

- *Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.*

DFARS 252.204-7012(f): Access to additional information or equipment necessary for forensic analysis

- *Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.*

DFARS 252.204-7012(f): Access to additional information or equipment necessary for forensic analysis

- *Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.*

DFARS 252.204-7012(g): Cyber incident damage assessment activities

- *Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.*

DFARS 252.204-7012(l): Other safeguarding or reporting requirements

- *Other safeguarding or reporting requirements. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.*

DFARS 252.204-7012(l): Other safeguarding or reporting requirements

- *Other safeguarding or reporting requirements. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor’s responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.*

DFARS 252.204-7012(m): Subcontracts

- *The Contractor shall –*
  - *Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial products or commercial services, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer*

DFARS 252.204-7012(m): Subcontracts

- *The Contractor shall –*
  - *Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial products or commercial services, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer*

DFARS 252.204-7012(m): Subcontracts

- *The Contractor shall –*
  - *Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial products or commercial services, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer*

DFARS Interim Rules

- Published September 29, 2020
- Effective Date: November 30, 2020

DFARS 7019

DFARS 7020

DFARS 7021

DFARS Interim Rules

- Published September 29, 2020
- Effective Date: November 30, 2020

DFARS 7019

DFARS 7020

DFARS 252.204-7019: Notice of NIST SP 800-171 DoD Assessment Requirements

DFARS 252.204-7019(b): Requirement

- *Requirement. In order to be considered for award, if the Offeror is required to implement NIST SP 800–171, the Offeror shall have a current assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204–7020) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. The Basic, Medium, and High NIST SP 800–171 DoD Assessments are described in the NIST SP 800–171 DoD Assessment Methodology located at https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf .*

DFARS 252.204-7019(b): Requirement

- *Requirement. In order to be considered for award, if the Offeror is required to implement NIST SP 800–171, the Offeror shall have a current assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204–7020) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. The Basic, Medium, and High NIST SP 800–171 DoD Assessments are described in the NIST SP 800–171 DoD Assessment Methodology located at https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf .*

DFARS 252.204-7019(c): Procedures

- *The Offeror shall verify that summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) are posted in the Supplier Performance Risk System (SPRS) () for all covered contractor information systems relevant to the offer.*

DFARS 252.204-7019(c): Procedures

- *The Offeror shall verify that summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) are posted in the Supplier Performance Risk System (SPRS) () for all covered contractor information systems relevant to the offer.*

DFARS 252.204-7019(d): Summary level scores

System Security Plan					

The absence of a system security plan would result in a finding that 'an assessment could not be completed due to incomplete information and noncompliance with DFARS clause 252.204-7012.'

DFARS 252.204-7019(d): Summary level scores

System Security Plan	CAGE Codes supported by this plan				

All industry CAGE code(s) associated with the information system(s) addressed by the system security plan

DFARS 252.204-7019(d): Summary level scores

System Security Plan	CAGE Codes supported by this plan	Brief description of the plan architecture			

A brief description of the system security plan architecture, if more than one plan exists

DFARS 252.204-7019(d): Summary level scores

System Security Plan	CAGE Codes supported by this plan	Brief description of the plan architecture	Date of assessment		

Date self-assessment was completed

DFARS 252.204-7019(d): Summary level scores

System Security Plan	CAGE Codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total Score	

Summary level score (e.g., 95 out of 110, NOT The individual value for each requirement)

Scores can go as low as -203

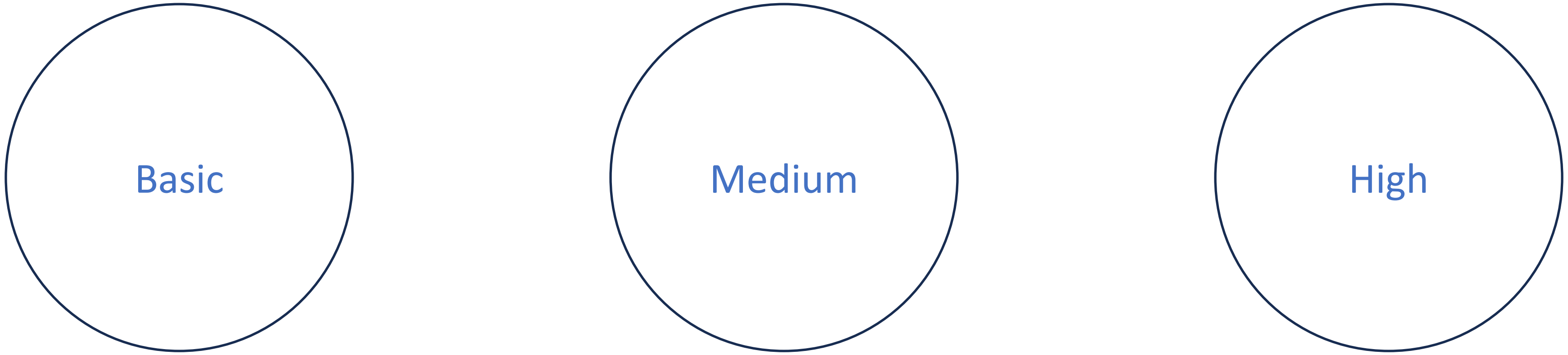
DFARS 252.204-7019(d): Summary level scores

System Security Plan	CAGE Codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total Score	Date score of 110 will be achieved

Date all requirements are expected to be implemented

DFARS 252.204-7020: NIST SP 800-171 DoD Assessment Requirements

DFARS 252.204-7020: NIST SP 800-171 DoD Assessment Requirements

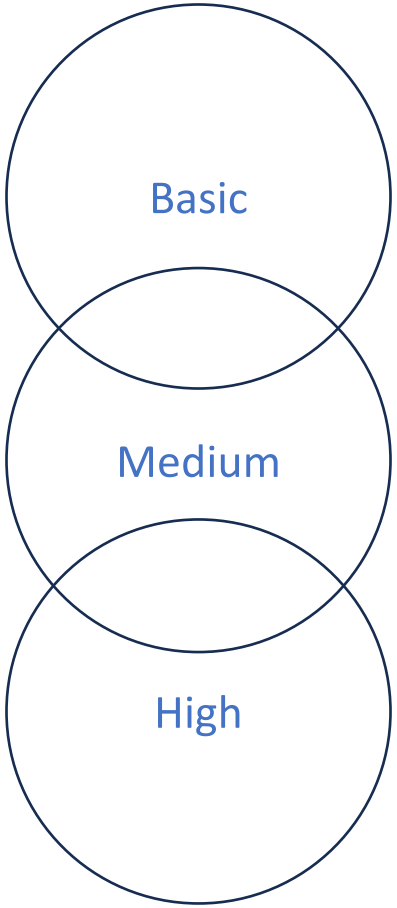


Basic

Medium

High

DFARS 252.204-7020: NIST SP 800-171 DoD Assessment Requirements



DFARS 252.204-7020(A): Definitions

- *Basic Assessment” means a contractor’s self-assessment of the contractor’s implementation of NIST SP 800-171 that—*
- *(1) Is based on the Contractor’s review of their system security plan(s) associated with covered contractor information system(s);*
- *(2) Is conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology; and*
- *(3) Results in a confidence level of “Low” in the resulting score, because it is a self-generated score.*

DFARS 252.204-7020(A): Definitions

- *Basic Assessment" means a contractor's self-assessment of the contractor's implementation of NIST SP 800-171 that—*
  - *(1) Is based on the Contractor's review of their system security plan(s) associated with covered contractor information system(s);*
  - *(2) Is conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology; and*
  - *(3) Results in a confidence level of "Low" in the resulting score, because it is a self-generated score.*

DFARS 252.204-7020(A): Definitions

- *“Medium Assessment” means an assessment conducted by the Government that—*
  - *(1) Consists of—*
  - *(i) A review of a contractor’s Basic Assessment;*
  - *(ii) A thorough document review; and*
  - *(iii) Discussions with the contractor to obtain additional information or clarification, as needed; and*
  - *(2) Results in a confidence level of “Medium” in the resulting score.*

DFARS 252.204-7020(A): Definitions

- *“Medium Assessment” means an assessment conducted by the Government that—*
  - *(1) Consists of—*
  - *(i) A review of a contractor’s Basic Assessment;*
  - *(ii) A thorough document review; and*
  - *(iii) Discussions with the contractor to obtain additional information or clarification, as needed; and*
  - *(2) Results in a confidence level of “Medium” in the resulting score.*

DFARS 252.204-7020(A): Definitions

- *“High Assessment” means an assessment that is conducted by Government personnel using NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information that—*
  - *(1) Consists of—*
  - *(i) A review of a contractor’s Basic Assessment;*
  - *(ii) A thorough document review;*
  - *(iii) Verification, examination, and demonstration of a Contractor’s system security plan to validate that NIST SP 800-171 security requirements have been implemented as described in the contractor’s system security plan; and*
  - *(iv) Discussions with the contractor to obtain additional information or clarification, as needed; and*
  - *(2) Results in a confidence level of “High” in the resulting score.*

DFARS 252.204-7020(A): Definitions

- *"High Assessment" means an assessment that is conducted by Government personnel using NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information that—*
  - *(1) Consists of—*
    - *(i) A review of a contractor's Basic Assessment;*
    - *(ii) A thorough document review;*
    - *(iii) Verification, examination, and demonstration of a Contractor's system security plan to validate that NIST SP 800-171 security requirements have been implemented as described in the contractor's system security plan; and*
    - *(iv) Discussions with the contractor to obtain additional information or clarification, as needed; and*
  - *(2) Results in a confidence level of "High" in the resulting score.*

DFARS 252.204-7020(C): Requirements

- *Requirements. The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800–171 DoD Assessment, as described in NIST SP 800–171 DoD Assessment Methodology at https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf , if necessary.*

DFARS 252.204-7020(C): Requirements

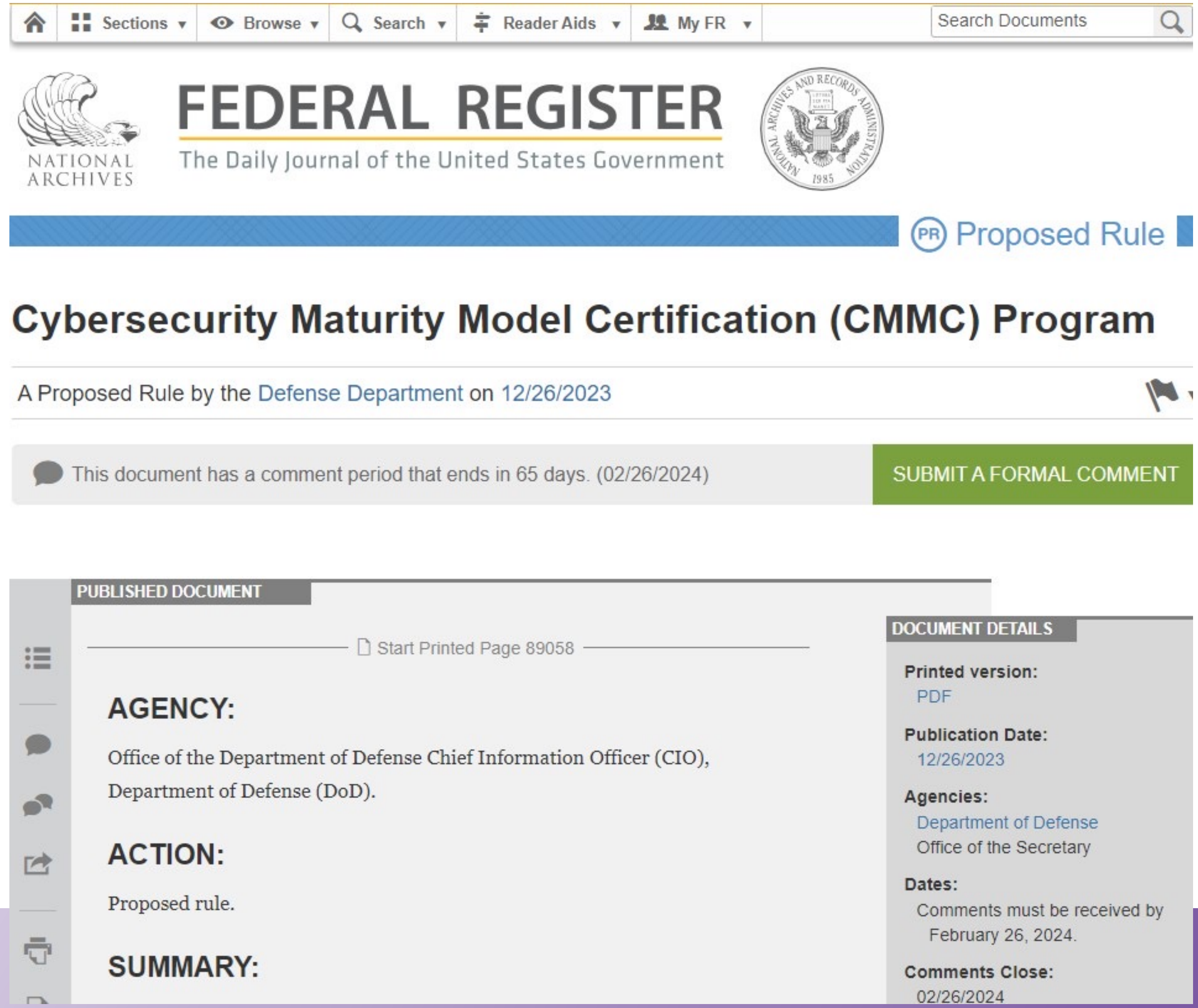
- *Requirements. The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800–171 DoD Assessment, as described in NIST SP 800–171 DoD Assessment Methodology at https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf , if necessary.*

DFARS 252.204-7021: NIST SP 800-171 DoD Assessment Requirements

DFARS 252.204-7021: Cybersecurity Maturity Model Certification Requirements

- *(b) Requirements. The Contractor shall have a current (i.e. not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.*

DFARS 252.204-7021: Cybersecurity Maturity Model Certification Requirements



FEDERAL REGISTER

The Daily Journal of the United States Government

Proposed Rule

Cybersecurity Maturity Model Certification (CMMC) Program

A Proposed Rule by the Defense Department on 12/26/2023

This document has a comment period that ends in 65 days. (02/26/2024)

SUBMIT A FORMAL COMMENT

PUBLISHED DOCUMENT

Start Printed Page 89058

AGENCY:

Office of the Department of Defense Chief Information Officer (CIO), Department of Defense (DoD).

ACTION:

Proposed rule.

SUMMARY:

DOCUMENT DETAILS

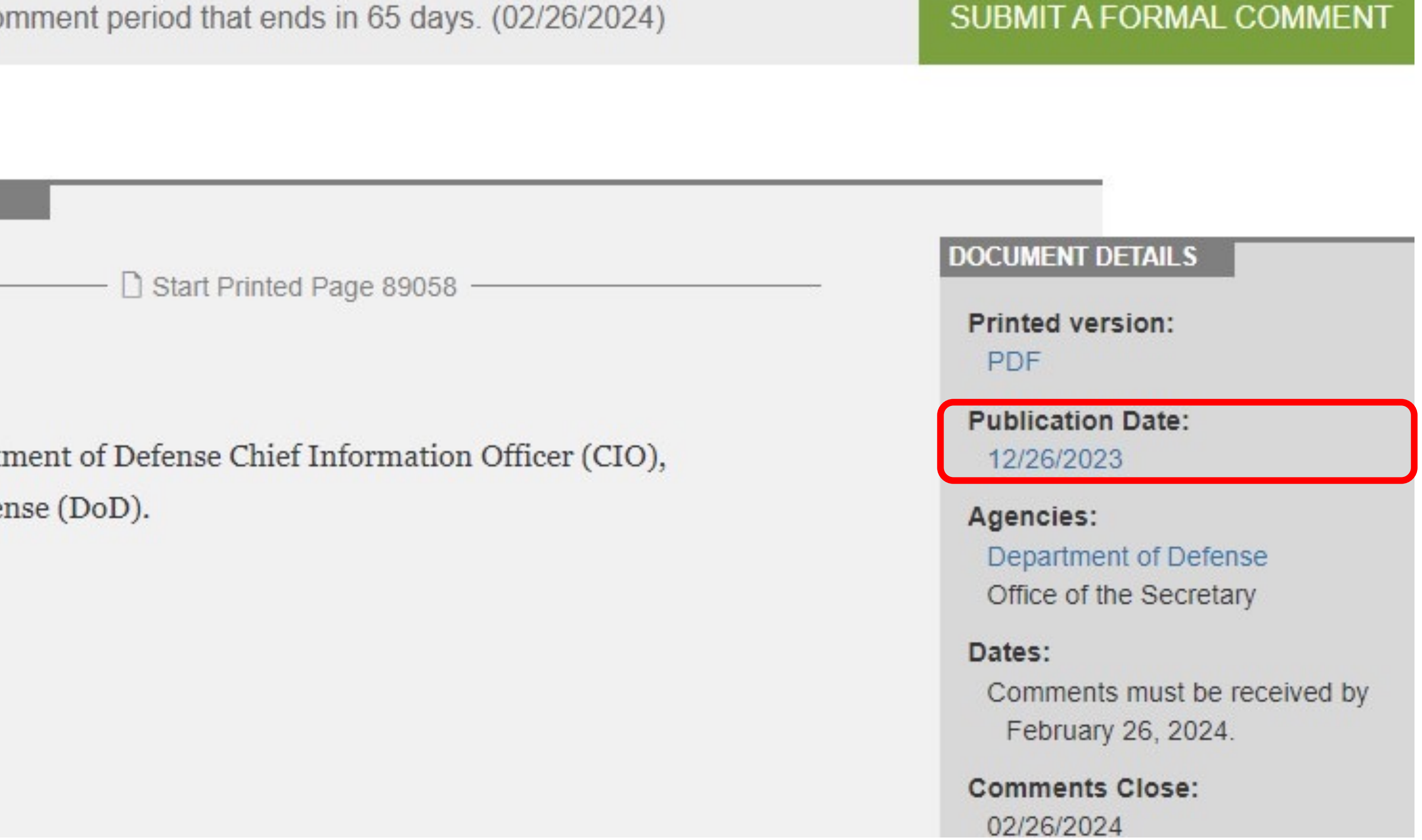
Printed version:
PDF

Publication Date:
12/26/2023

Agencies:
Department of Defense
Office of the Secretary

Dates:
Comments must be received by February 26, 2024.

Comments Close:
02/26/2024



mment period that ends in 65 days. (02/26/2024)

Start Printed Page 89058

ment of Defense Chief Information Officer (CIO),
nse (DoD).

DOCUMENT DETAILS

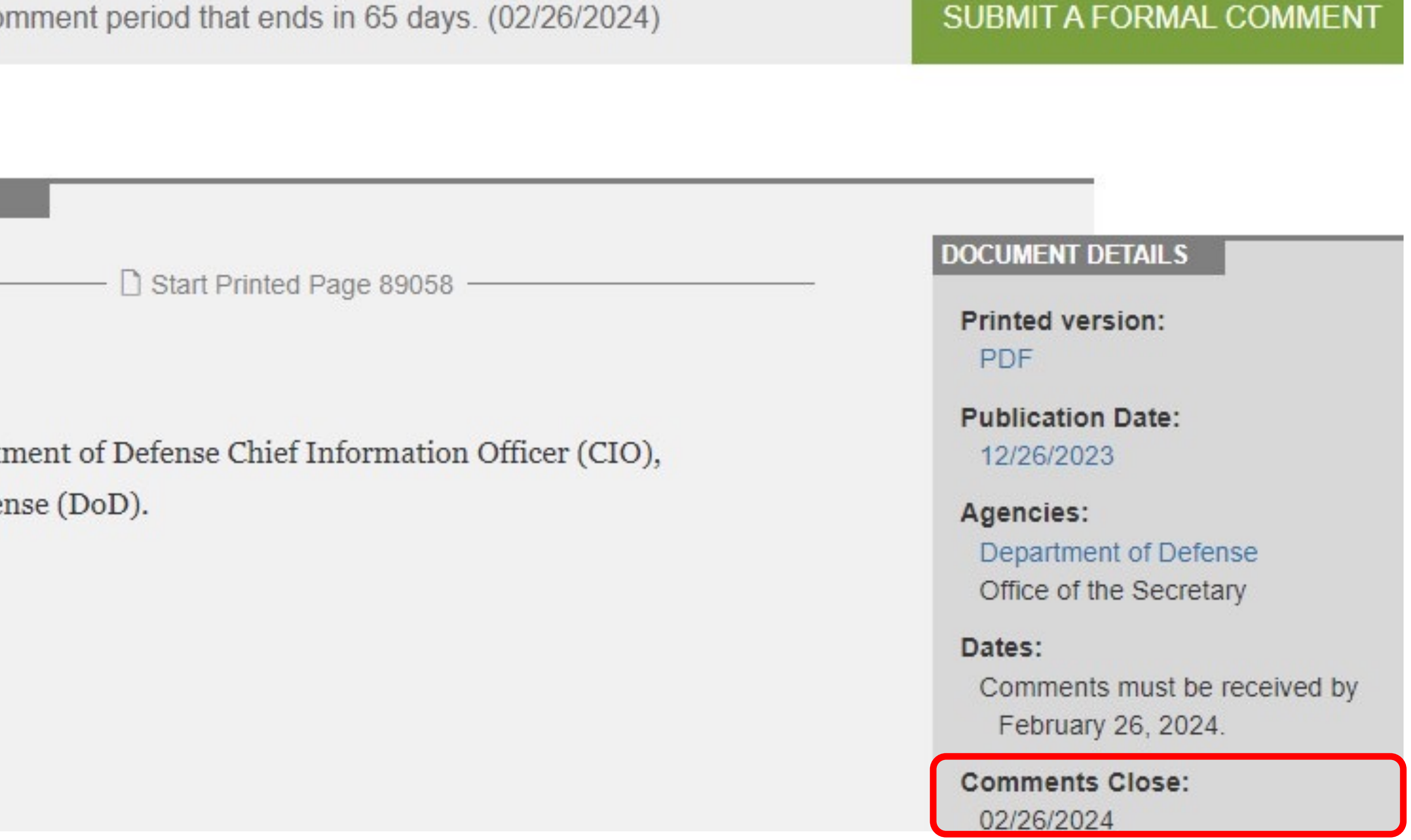
Printed version:
PDF

Publication Date:
12/26/2023

Agencies:
Department of Defense
Office of the Secretary

Dates:
Comments must be received by February 26, 2024.

Comments Close:
02/26/2024



omment period that ends in 65 days. (02/26/2024)

SUBMIT A FORMAL COMMENT

Start Printed Page 89058

ment of Defense Chief Information Officer (CIO),
ense (DoD).

DOCUMENT DETAILS

Printed version:
PDF

Publication Date:
12/26/2023

Agencies:
Department of Defense
Office of the Secretary

Dates:
Comments must be received by February 26, 2024.

Comments Close:
02/26/2024

David McKeown, DoD Senior Information Security Officer & Deputy Chief Information Officer

- *"We're targeting late fall of next year (2024) so that can start to be put into contracts."*

May 23, 2023

2023 Cyber Summit

Tim Gorman, Pentagon Spokesperson

- *"…DoD would like to thank all the companies who have taken the time to provide comments on the CMMC rule to date; however, we do not intend to extend the public comment period at this time."*
- *"We have already begun the adjudication process and will move to the next step rapidly after the close of the comment window."*

February 8, 2024

DFARS 252.204-7024: Notice on the use of the Supplier Performance Risk System

DFARS 252.204-7024: Notice on the use of the Supplier Performance Risk System

- *(c) The Contracting Officer will consider SPRS risk assessments during the evaluation of quotations or offers received in response to this solicitation as follows:*
    - *Item risk will be considered to determine whether the procurement represents a high performance risk to the Government.*
    - *Price risk will be considered in determining if a proposed price is consistent with historical prices paid for a product or a service or otherwise creates a risk to the Government.*
    - *Supplier risk, including but not limited to quality and delivery, will be considered to assess the risk of unsuccessful performance and supply chain risk.*

DFARS 252.204-7024: Notice on the use of the Supplier Performance Risk System

- *(c) The Contracting Officer will consider SPRS risk assessments during the evaluation of quotations or offers received in response to this solicitation as follows:*
  - *Item risk will be considered to determine whether the procurement represents a high performance risk to the Government.*
  - *Price risk will be considered in determining if a proposed price is consistent with historical prices paid for a product or a service or otherwise creates a risk to the Government.*
  - *Supplier risk, including but not limited to quality and delivery, will be considered to assess the risk of unsuccessful performance and supply chain risk.*

Top Misunderstood Requirements

Top Misunderstood Requirements

3.1.22

3.3.1	3.5.3
3.3.3	3.7.3
3.4.3	3.8.3

NIST SP 800-171 Paragraph 1.1: Purpose and Applicability

- *The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.*

NIST SPECIAL PUBLICATION
SP 800-171
171
REVISION 2
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

NIST SP 800-171 Paragraph 1.1: Purpose and Applicability

- *The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.*

NIST SPECIAL PUBLICATION
SP 800-171
171
REVISION 2
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

NIST SP 800-171 Paragraph 1.1: Purpose and Applicability

- *System components include, for example: mainframes, workstations, servers; input and output devices; network components; operating systems; virtual machines; and applications.*

NIST SPECIAL PUBLICATION

SP 800-171

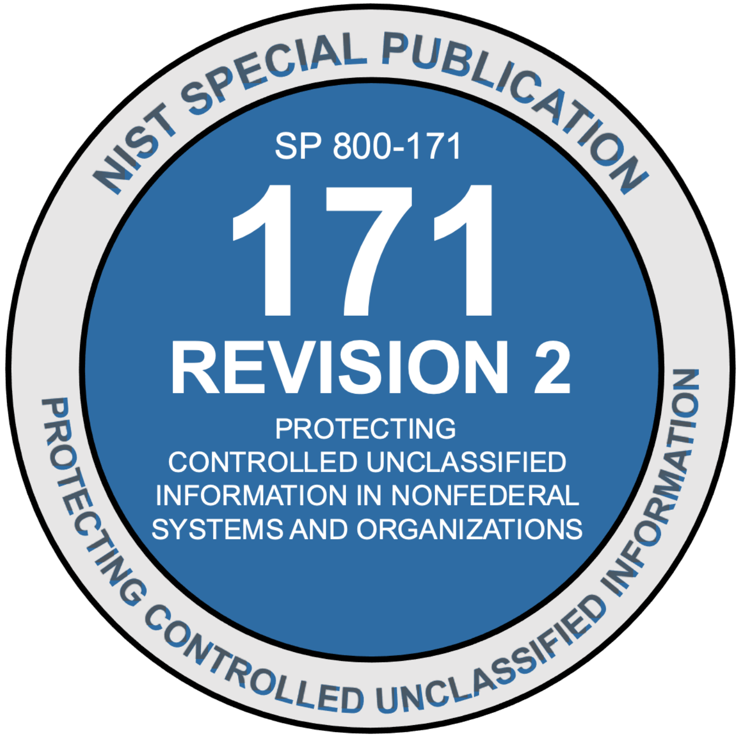
171

REVISION 2

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS

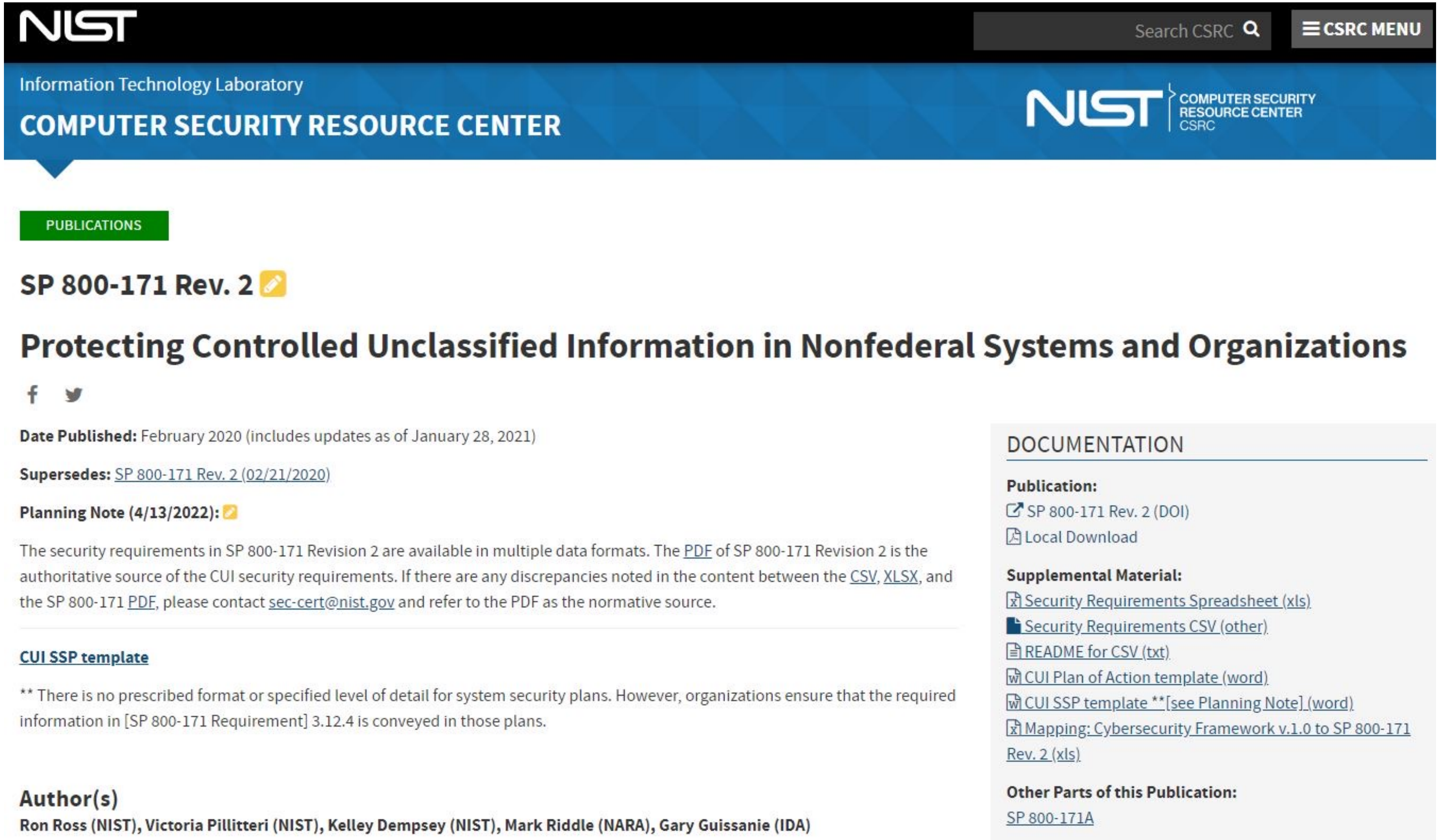
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

NIST SP 800-171 versus NIST SP 800-171A


NIST SPECIAL PUBLICATION
SP 800-171
171
REVISION 2
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

NIST SPECIAL PUBLICATION
SP 800-171A
171A
ASSESSING SECURITY REQUIREMENTS FOR CONTROLLED UNCLASSIFIED INFORMATION
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

NIST SP 800-171 versus NIST SP 800-171A


NIST
Search CSRC
CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC
PUBLICATIONS

SP 800-171 Rev. 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Date Published: February 2020 (includes updates as of January 28, 2021)

Supersedes: SP 800-171 Rev. 2 (02/21/2020)

Planning Note (4/13/2022):

The security requirements in SP 800-171 Revision 2 are available in multiple data formats. The PDF of SP 800-171 Revision 2 is the authoritative source of the CUI security requirements. If there are any discrepancies noted in the content between the CSV, XLSX, and the SP 800-171 PDF, please contact sec-cert@nist.gov and refer to the PDF as the normative source.

CUI SSP template

** There is no prescribed format or specified level of detail for system security plans. However, organizations ensure that the required information in [SP 800-171 Requirement] 3.12.4 is conveyed in those plans.

Author(s)

Ron Ross (NIST), Victoria Pillitteri (NIST), Kelley Dempsey (NIST), Mark Riddle (NARA), Gary Guissanie (IDA)

DOCUMENTATION

Publication:

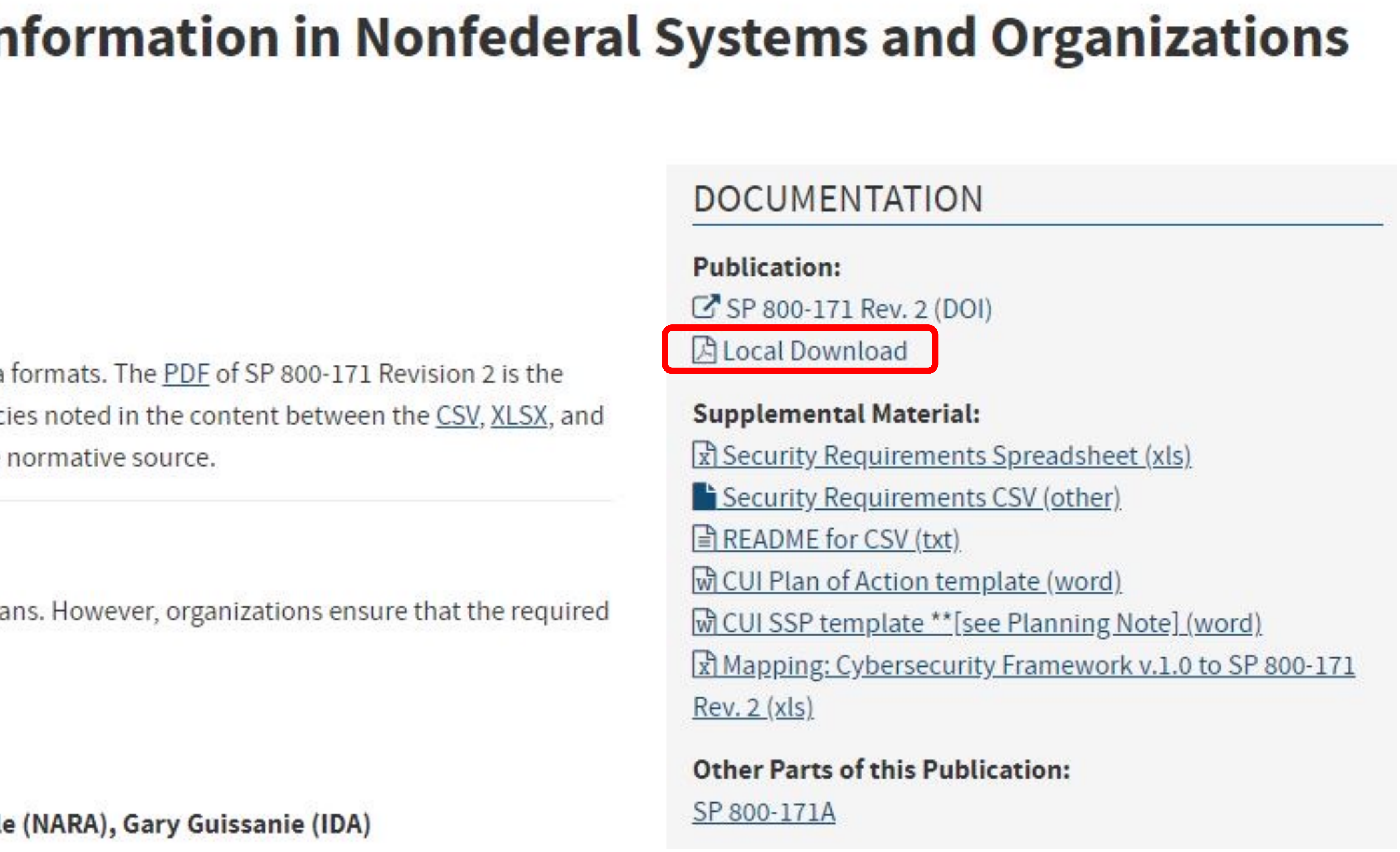
- SP 800-171 Rev. 2 (DOI)
- Local Download

Supplemental Material:

- Security Requirements Spreadsheet (xls)
- Security Requirements CSV (other)
- README for CSV (txt)
- CUI Plan of Action template (word)
- CUI SSP template **[see Planning Note] (word)
- Mapping: Cybersecurity Framework v.1.0 to SP 800-171 Rev. 2 (xls)

Other Parts of this Publication:

SP 800-171A



nformation in Nonfederal Systems and Organizations

a formats. The PDF of SP 800-171 Revision 2 is the
cies noted in the content between the CSV, XLSX, and
normative source.

ans. However, organizations ensure that the required

le (NARA), Gary Guissanie (IDA)

DOCUMENTATION

Publication:

SP 800-171 Rev. 2 (DOI)

Local Download

Supplemental Material:

Security Requirements Spreadsheet (xls)

Security Requirements CSV (other)

README for CSV (txt)

CUI Plan of Action template (word)

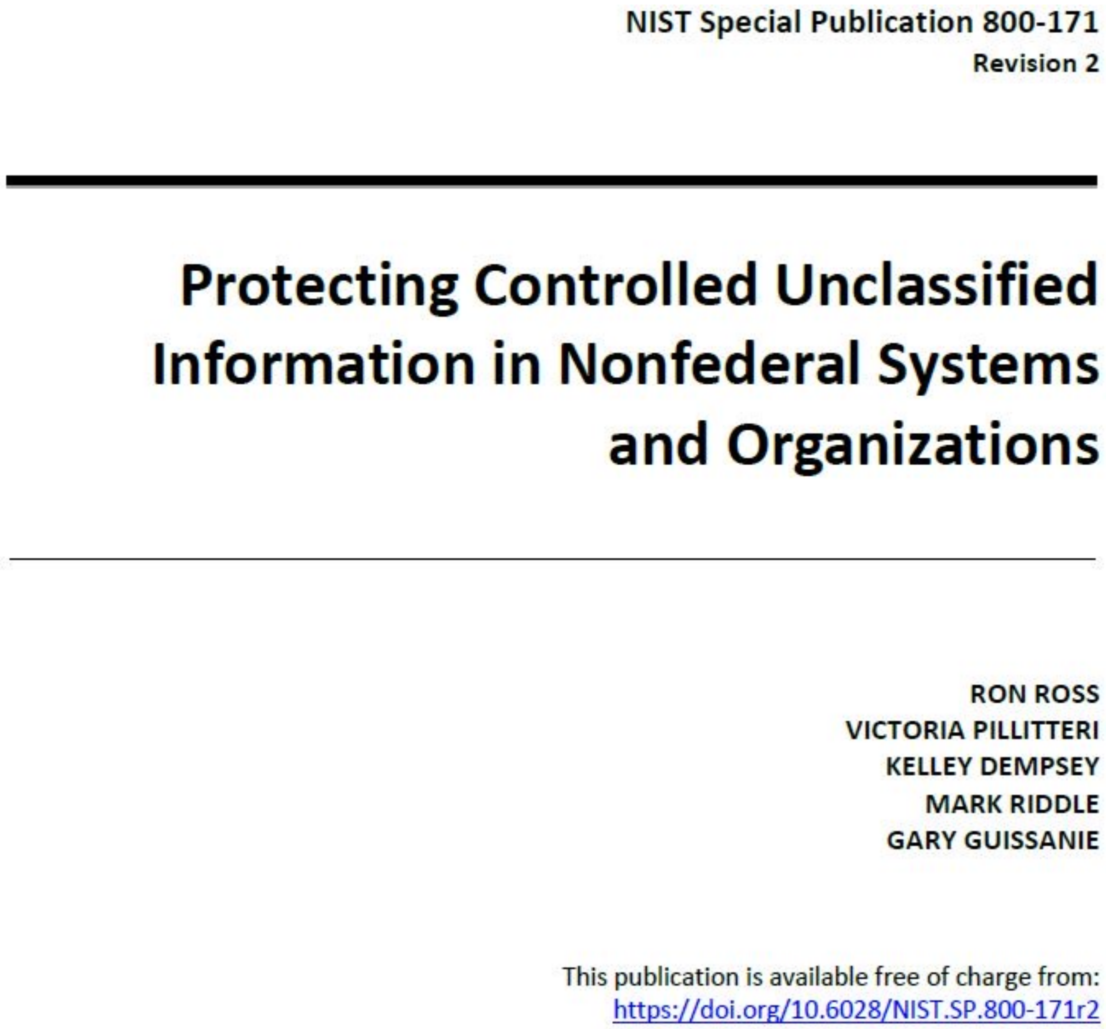
CUI SSP template **[see Planning Note] (word)

Mapping: Cybersecurity Framework v.1.0 to SP 800-171 Rev. 2 (xls)

Other Parts of this Publication:

SP 800-171A

NIST SP 800-171 versus NIST SP 800-171A



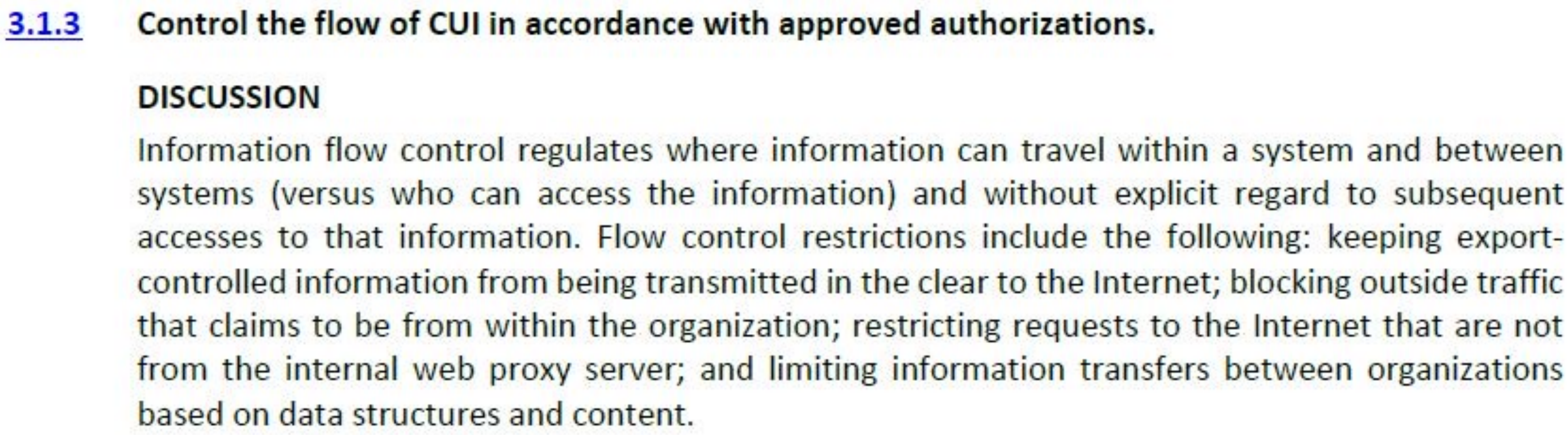
NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

NIST SP 800-171 versus NIST SP 800-171A

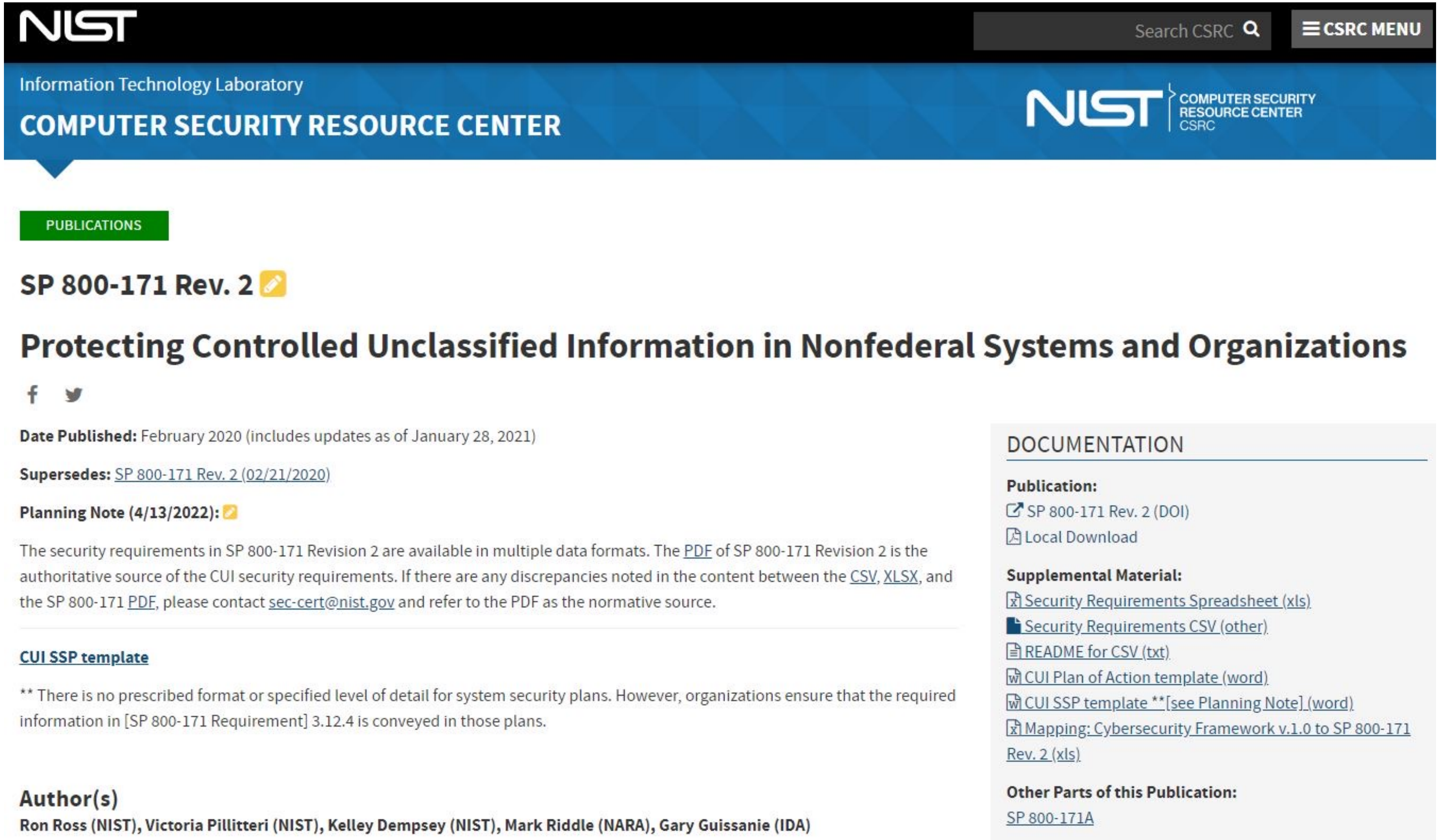


3.1.3 Control the flow of CUI in accordance with approved authorizations.

DISCUSSION

Information flow control regulates where information can travel within a system and between systems (versus who can access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include the following: keeping export-controlled information from being transmitted in the clear to the Internet; blocking outside traffic that claims to be from within the organization; restricting requests to the Internet that are not from the internal web proxy server; and limiting information transfers between organizations based on data structures and content.

NIST SP 800-171 versus NIST SP 800-171A



NIST
Search CSRC
☰ CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC
PUBLICATIONS

SP 800-171 Rev. 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Date Published: February 2020 (includes updates as of January 28, 2021)

Supersedes: SP 800-171 Rev. 2 (02/21/2020)

Planning Note (4/13/2022):

The security requirements in SP 800-171 Revision 2 are available in multiple data formats. The PDF of SP 800-171 Revision 2 is the authoritative source of the CUI security requirements. If there are any discrepancies noted in the content between the CSV, XLSX, and the SP 800-171 PDF, please contact sec-cert@nist.gov and refer to the PDF as the normative source.

CUI SSP template

** There is no prescribed format or specified level of detail for system security plans. However, organizations ensure that the required information in [SP 800-171 Requirement] 3.12.4 is conveyed in those plans.

Author(s)

Ron Ross (NIST), Victoria Pillitteri (NIST), Kelley Dempsey (NIST), Mark Riddle (NARA), Gary Guissanie (IDA)

DOCUMENTATION

Publication:

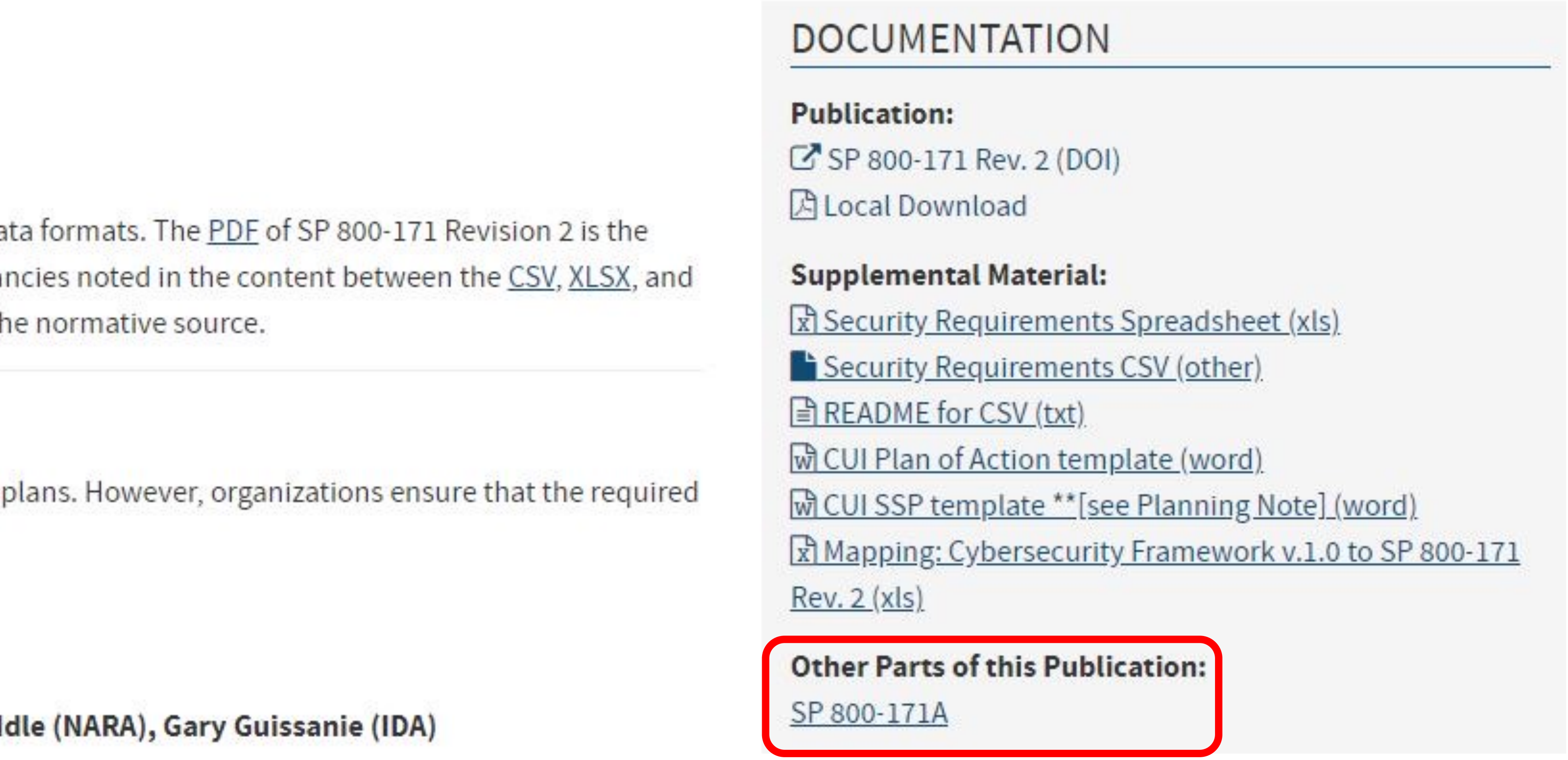
SP 800-171 Rev. 2 (DOI)
Local Download

Supplemental Material:

Security Requirements Spreadsheet (xls)
Security Requirements CSV (other)
README for CSV (txt)
CUI Plan of Action template (word)
CUI SSP template **[see Planning Note] (word)
Mapping: Cybersecurity Framework v.1.0 to SP 800-171 Rev. 2 (xls)

Other Parts of this Publication:

SP 800-171A



ata formats. The PDF of SP 800-171 Revision 2 is the
ncies noted in the content between the CSV, XLSX, and
he normative source.

plans. However, organizations ensure that the required

dle (NARA), Gary Guissanie (IDA)

DOCUMENTATION

Publication:

SP 800-171 Rev. 2 (DOI)

Local Download

Supplemental Material:

Security Requirements Spreadsheet (xls)

Security Requirements CSV (other)

README for CSV (txt)

CUI Plan of Action template (word)

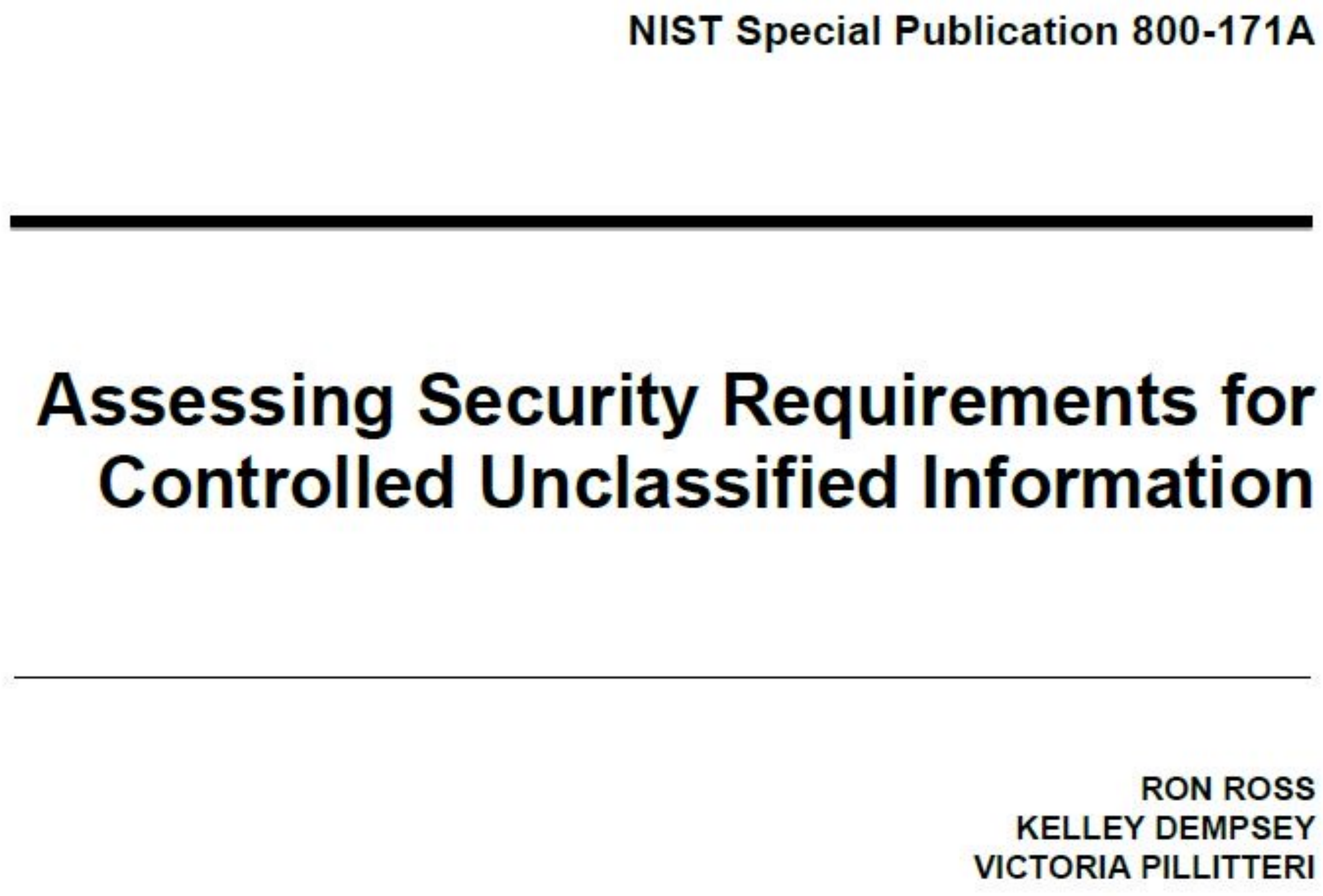
CUI SSP template **[see Planning Note] (word)

Mapping: Cybersecurity Framework v.1.0 to SP 800-171 Rev. 2 (xls)

Other Parts of this Publication:

SP 800-171A

NIST SP 800-171 versus NIST SP 800-171A

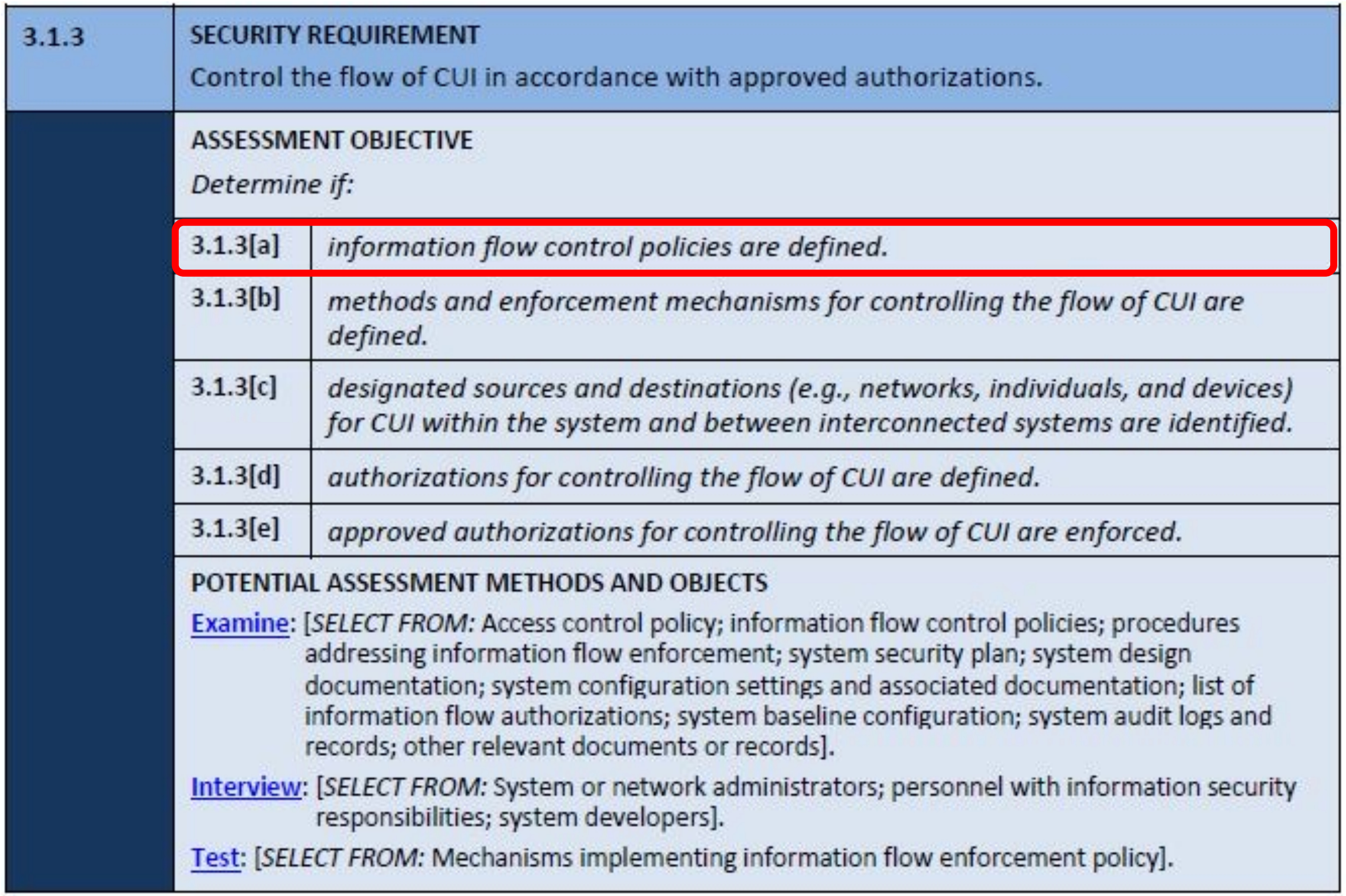


NIST Special Publication 800-171A

Assessing Security Requirements for Controlled Unclassified Information

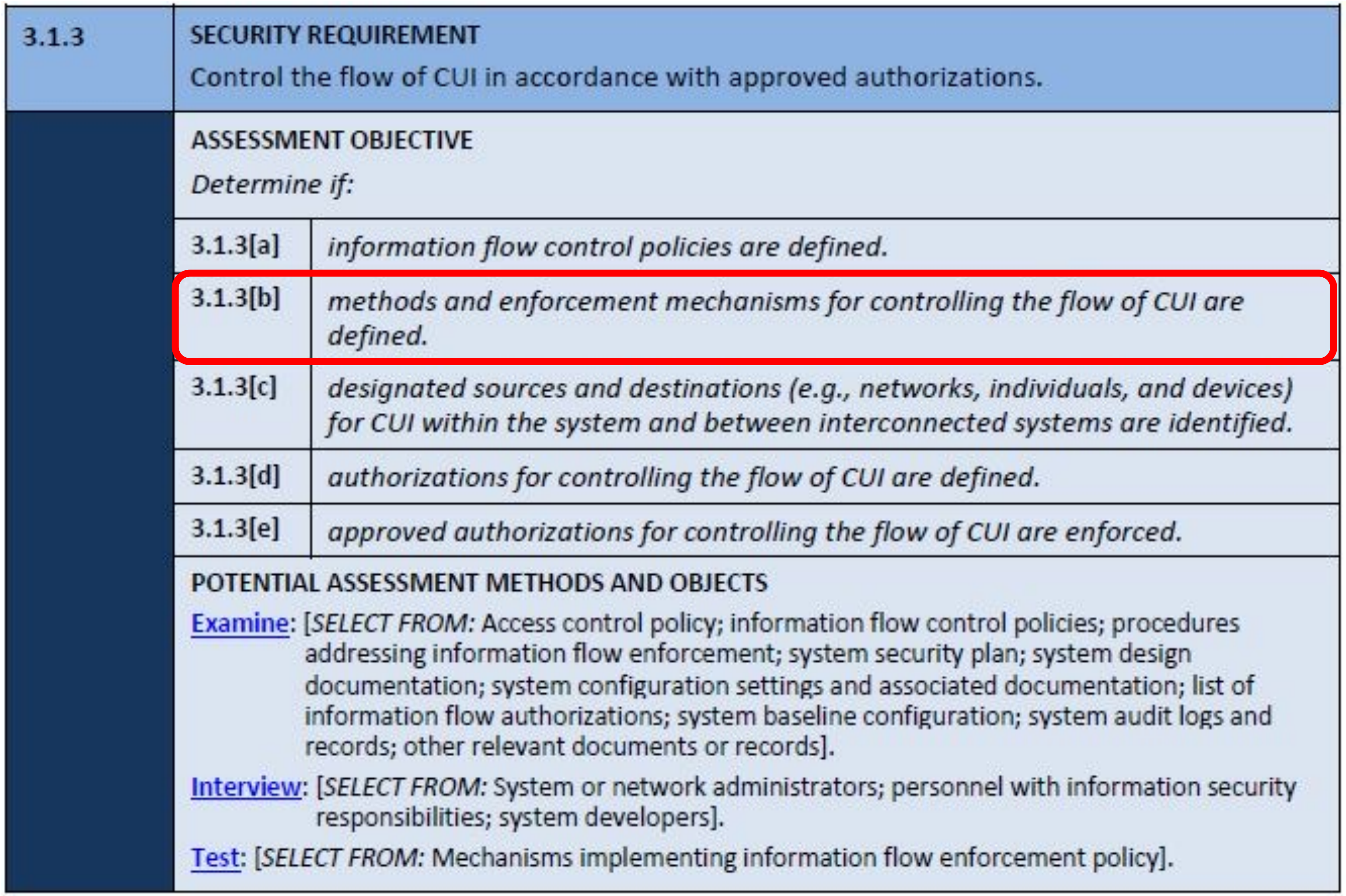
RON ROSS
KELLEY DEMPSEY
VICTORIA PILLITTERI

NIST SP 800-171 versus NIST SP 800-171A



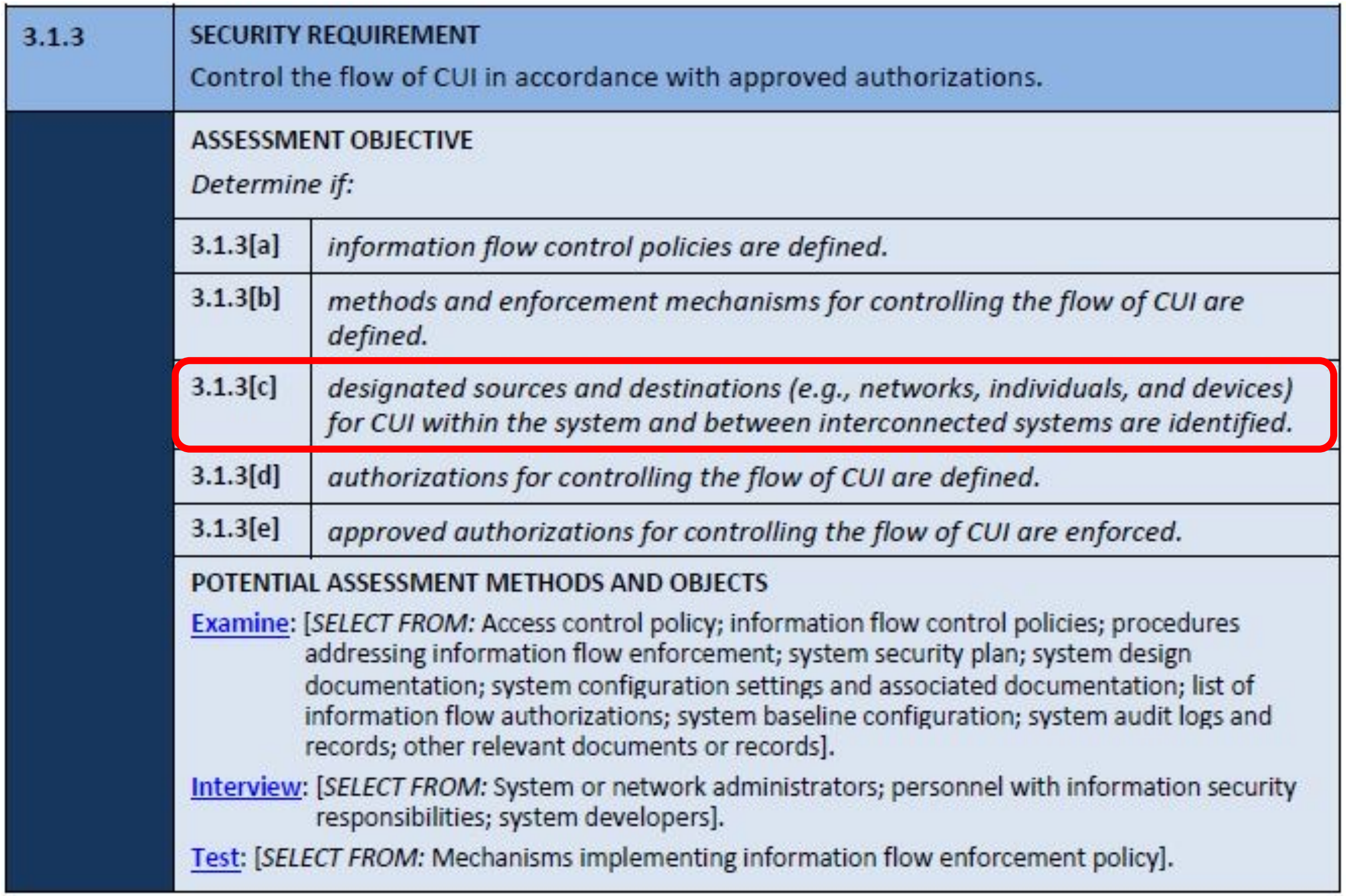
3.1.3	SECURITY REQUIREMENT Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].	

NIST SP 800-171 versus NIST SP 800-171A



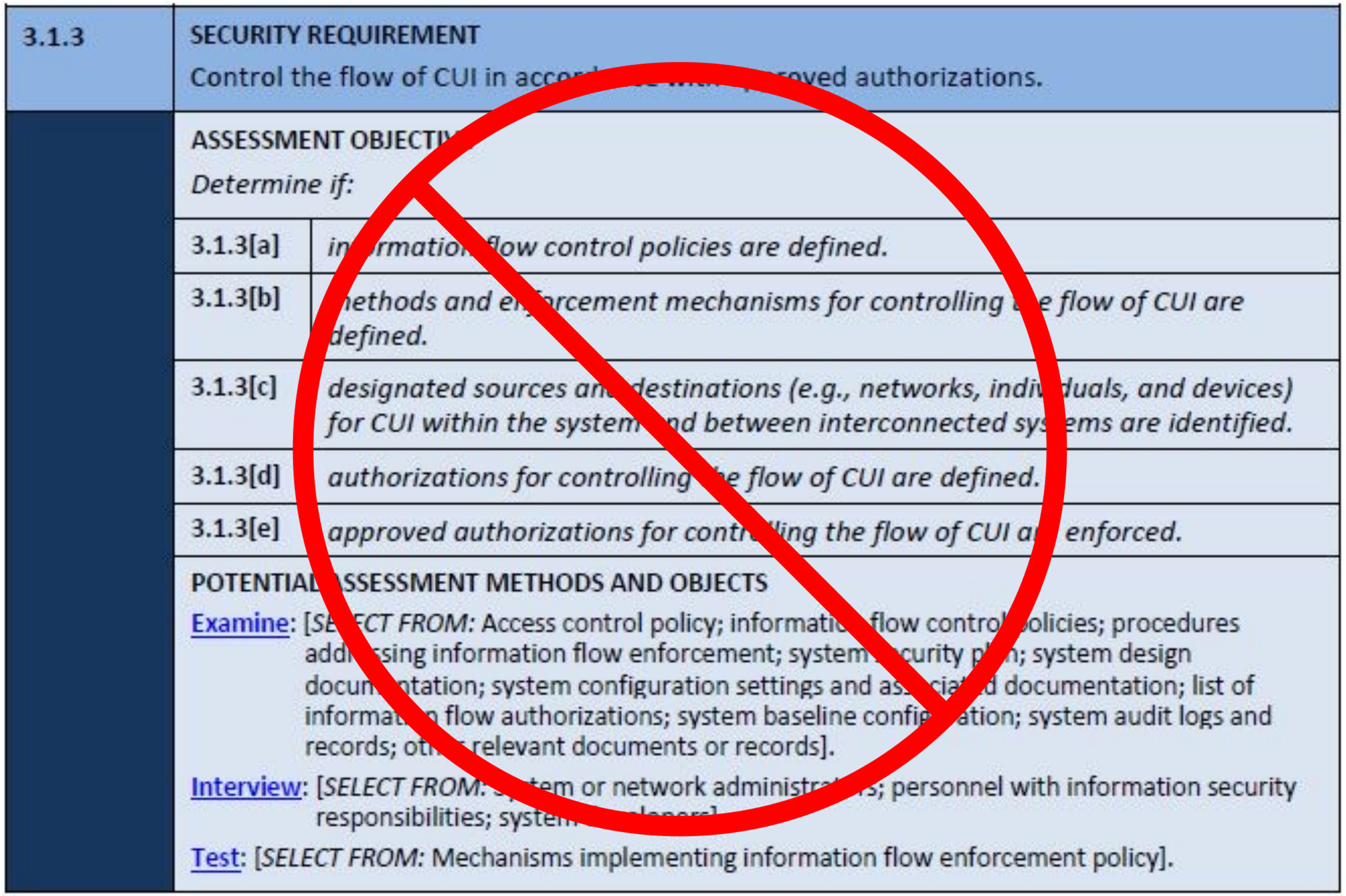
3.1.3	SECURITY REQUIREMENT Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].	

NIST SP 800-171 versus NIST SP 800-171A



3.1.3	SECURITY REQUIREMENT Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].	

NIST SP 800-171 versus NIST SP 800-171A



3.1.3	SECURITY REQUIREMENT Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].	

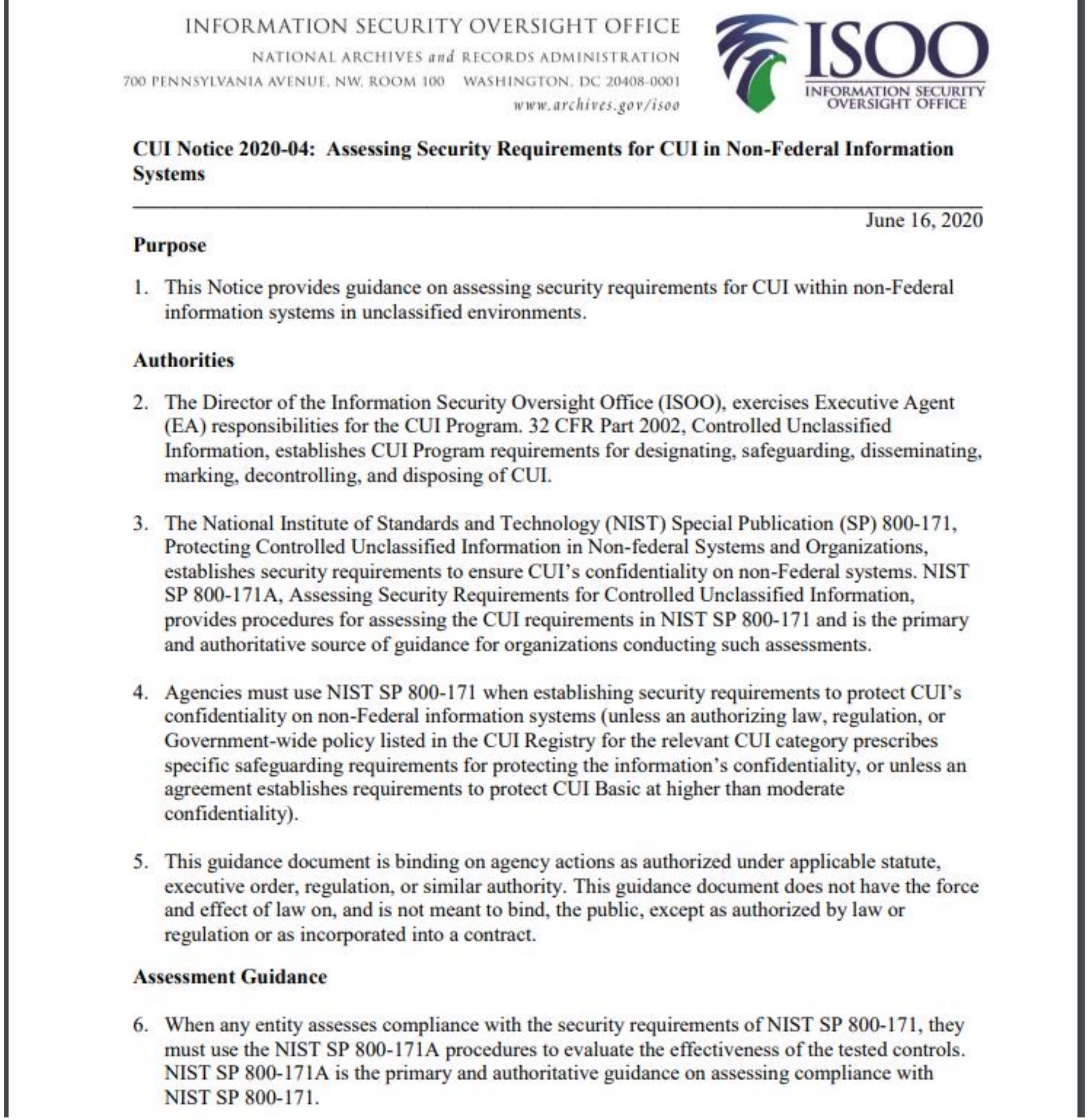
NIST SP 800-171 versus NIST SP 800-171A

- 110 requirements

- 320 assessment objectives

NIST SPECIAL PUBLICATION
SP 800-171
171
REVISION 2
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

NIST SPECIAL PUBLICATION
SP 800-171A
171A
ASSESSING SECURITY REQUIREMENTS FOR CONTROLLED UNCLASSIFIED INFORMATION
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION



INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES *and* RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo

ISOO
INFORMATION SECURITY
OVERSIGHT OFFICE

CUI Notice 2020-04: Assessing Security Requirements for CUI in Non-Federal Information Systems

June 16, 2020

Purpose

1. This Notice provides guidance on assessing security requirements for CUI within non-Federal information systems in unclassified environments.

Authorities

2. The Director of the Information Security Oversight Office (ISOO), exercises Executive Agent (EA) responsibilities for the CUI Program. 32 CFR Part 2002, Controlled Unclassified Information, establishes CUI Program requirements for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI.

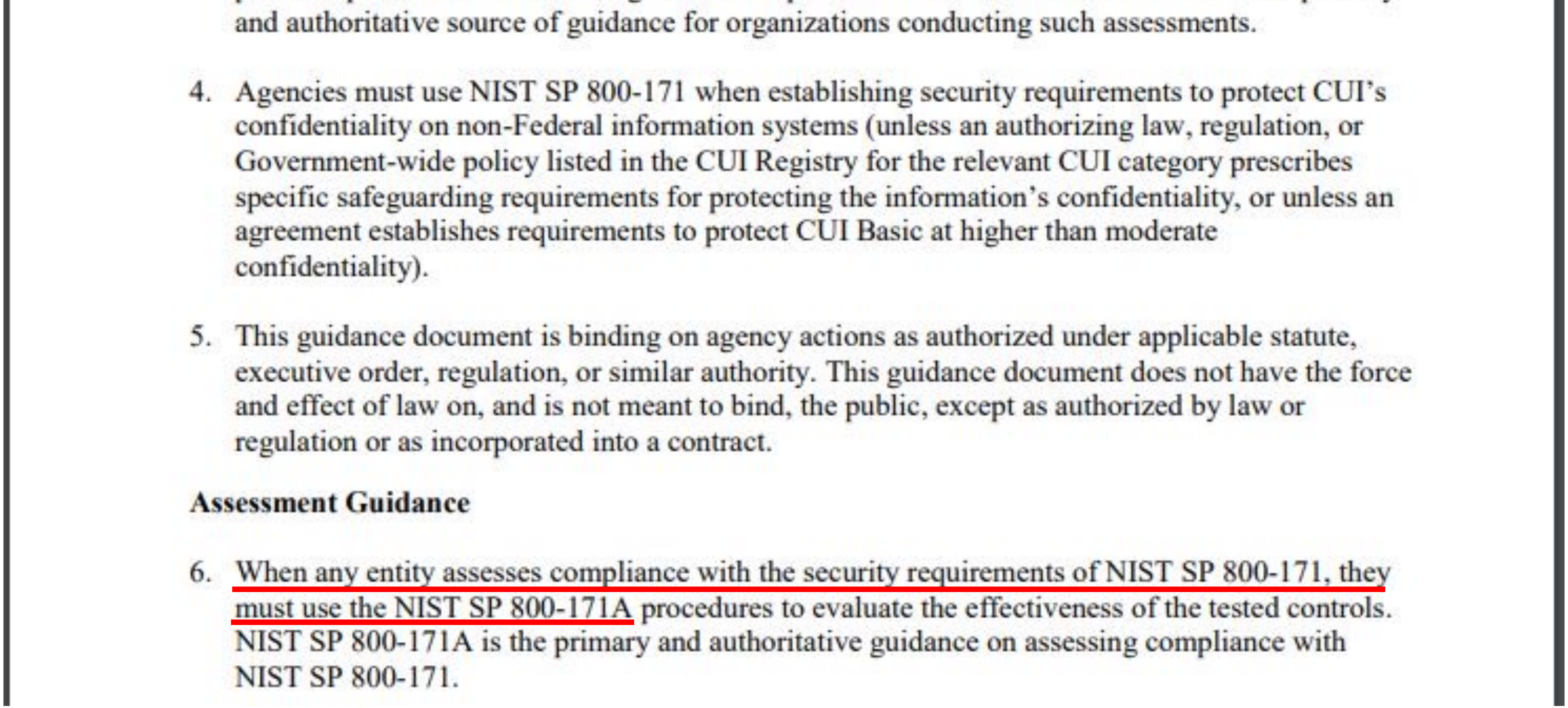
3. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Non-federal Systems and Organizations, establishes security requirements to ensure CUI's confidentiality on non-Federal systems. NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information, provides procedures for assessing the CUI requirements in NIST SP 800-171 and is the primary and authoritative source of guidance for organizations conducting such assessments.

4. Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems (unless an authorizing law, regulation, or Government-wide policy listed in the CUI Registry for the relevant CUI category prescribes specific safeguarding requirements for protecting the information's confidentiality, or unless an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality).

5. This guidance document is binding on agency actions as authorized under applicable statute, executive order, regulation, or similar authority. This guidance document does not have the force and effect of law on, and is not meant to bind, the public, except as authorized by law or regulation or as incorporated into a contract.

Assessment Guidance

6. When any entity assesses compliance with the security requirements of NIST SP 800-171, they must use the NIST SP 800-171A procedures to evaluate the effectiveness of the tested controls. NIST SP 800-171A is the primary and authoritative guidance on assessing compliance with NIST SP 800-171.



and authoritative source of guidance for organizations conducting such assessments.

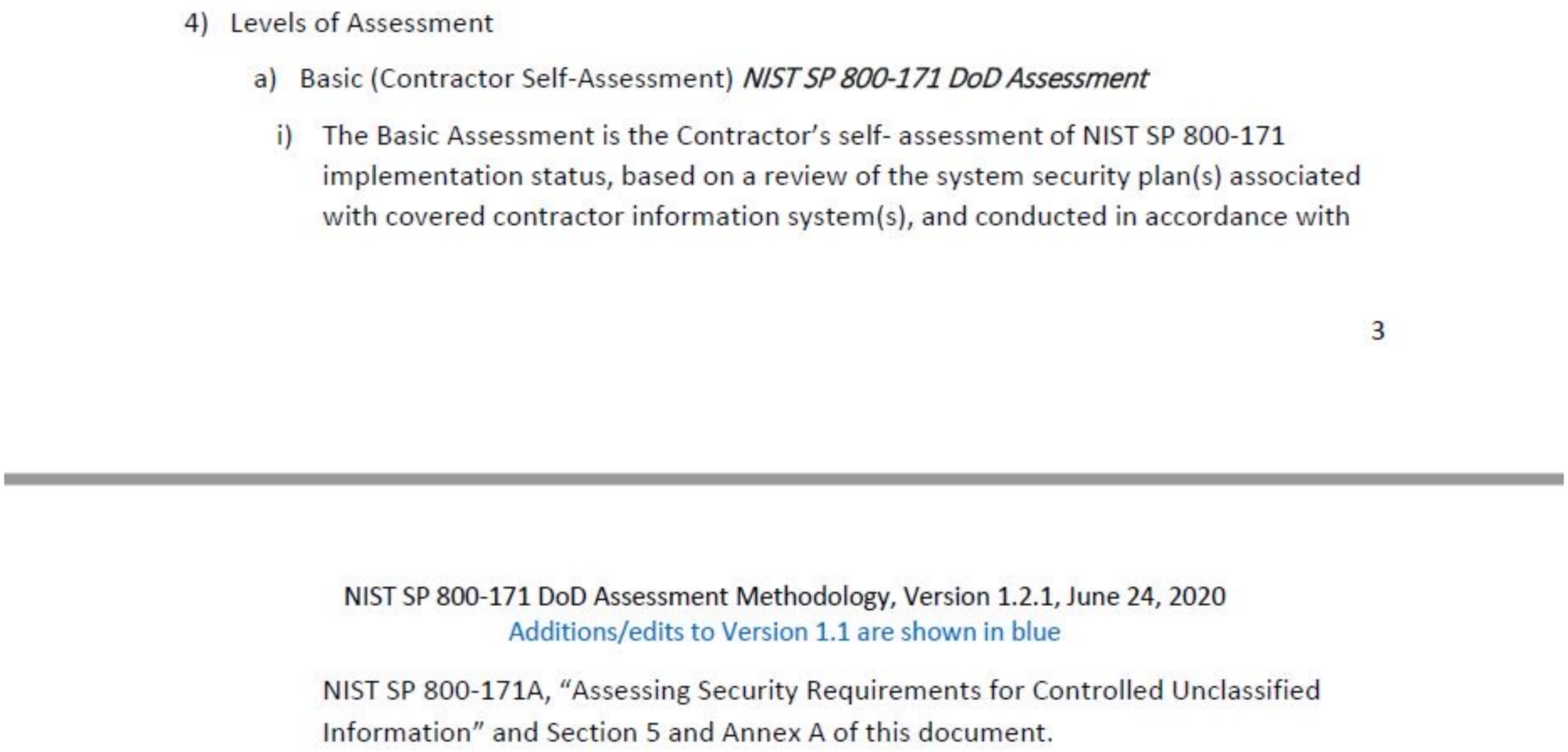
4. Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems (unless an authorizing law, regulation, or Government-wide policy listed in the CUI Registry for the relevant CUI category prescribes specific safeguarding requirements for protecting the information's confidentiality, or unless an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality).

5. This guidance document is binding on agency actions as authorized under applicable statute, executive order, regulation, or similar authority. This guidance document does not have the force and effect of law on, and is not meant to bind, the public, except as authorized by law or regulation or as incorporated into a contract.

Assessment Guidance

6. When any entity assesses compliance with the security requirements of NIST SP 800-171, they must use the NIST SP 800-171A procedures to evaluate the effectiveness of the tested controls. NIST SP 800-171A is the primary and authoritative guidance on assessing compliance with NIST SP 800-171.

DoD Assessment Methodology v1.2.1

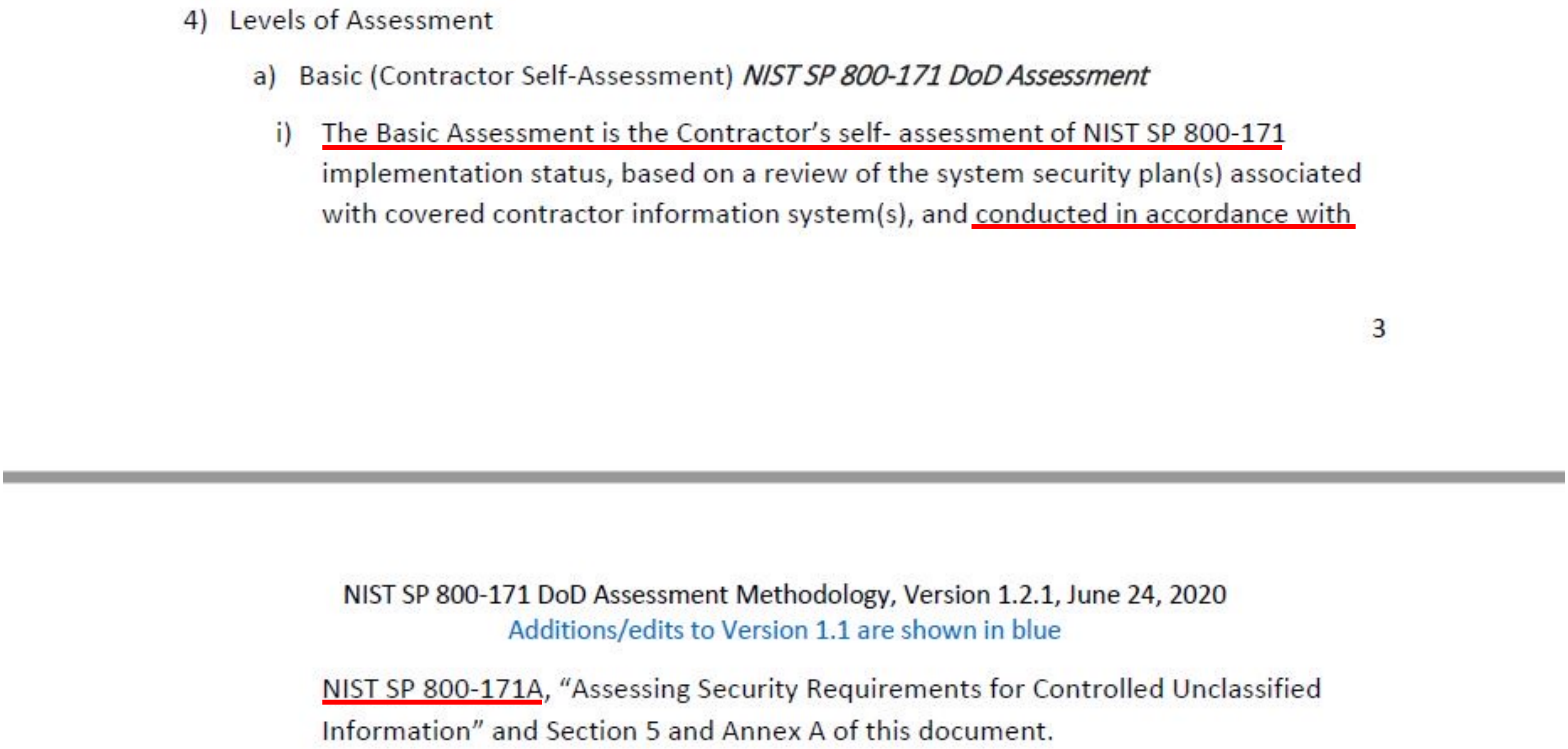


4) Levels of Assessment

a) Basic (Contractor Self-Assessment) *NIST SP 800-171 DoD Assessment*

i) The Basic Assessment is the Contractor's self- assessment of NIST SP 800-171 implementation status, based on a review of the system security plan(s) associated with covered contractor information system(s), and conducted in accordance with

NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information" and Section 5 and Annex A of this document.



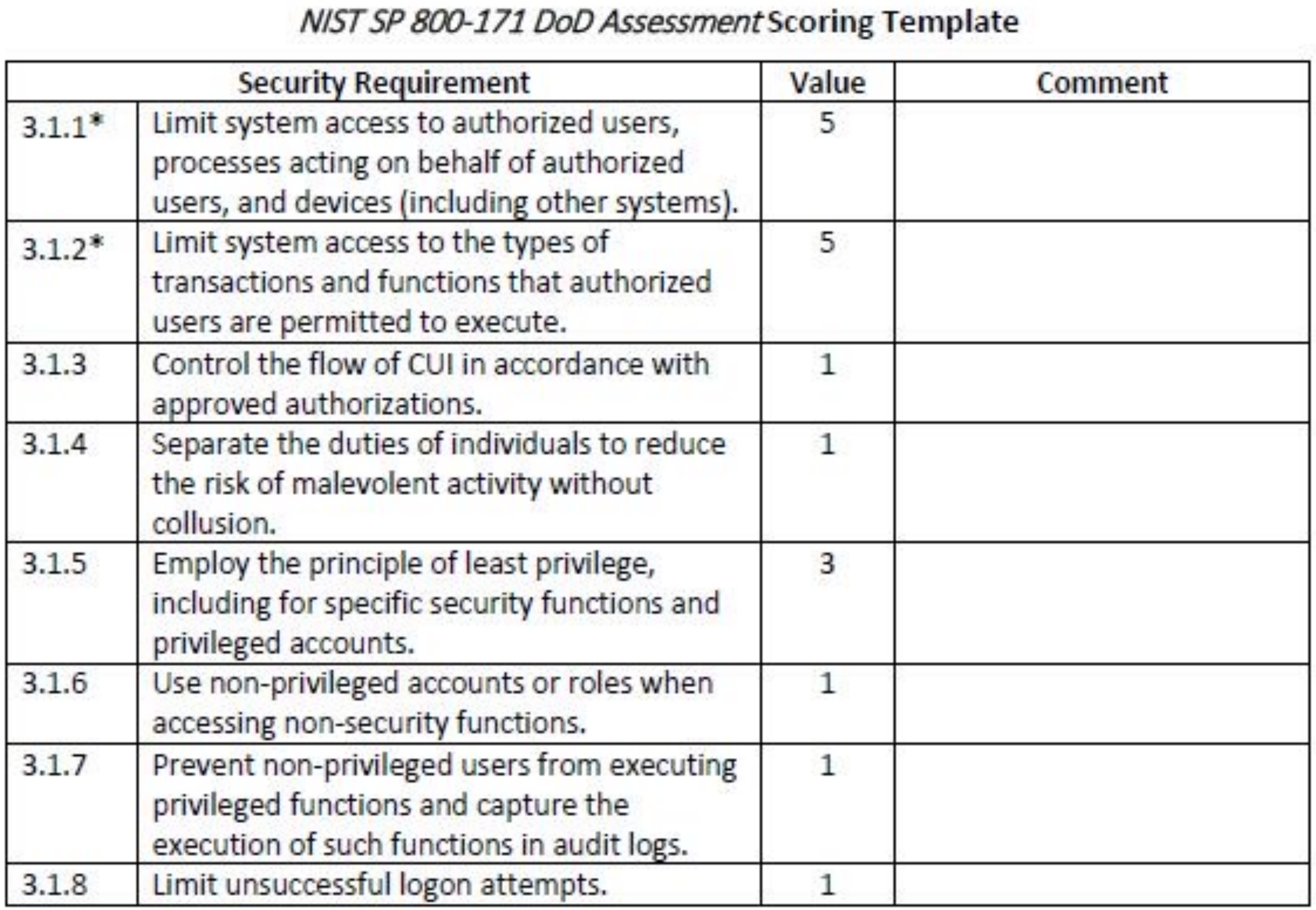
4) Levels of Assessment

a) Basic (Contractor Self-Assessment) *NIST SP 800-171 DoD Assessment*

i) The Basic Assessment is the Contractor's self- assessment of NIST SP 800-171 implementation status, based on a review of the system security plan(s) associated with covered contractor information system(s), and conducted in accordance with

NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information" and Section 5 and Annex A of this document.

DoD Assessment Methodology v1.2.1



NIST SP 800-171 DoD Assessment Scoring Template

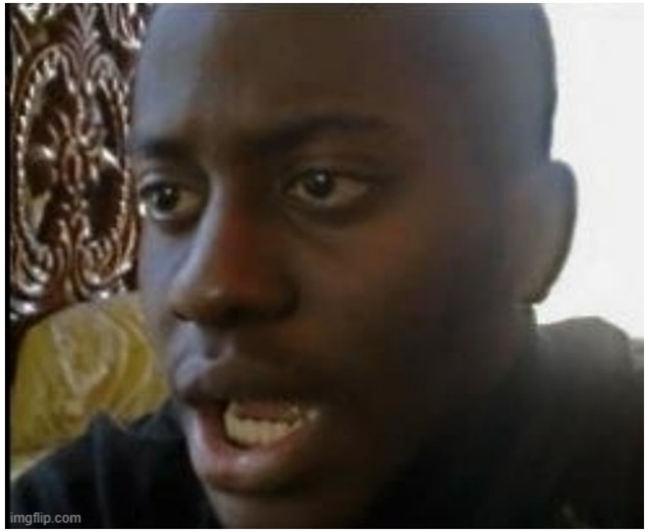
Security Requirement		Value	Comment
3.1.1*	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	5	
3.1.2*	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5	
3.1.3	Control the flow of CUI in accordance with approved authorizations.	1	
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3	
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	1	
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	1	
3.1.8	Limit unsuccessful logon attempts.	1	

DoD Assessment Methodology v1.2.1

110

DoD Assessment Methodology v1.2.1

-203



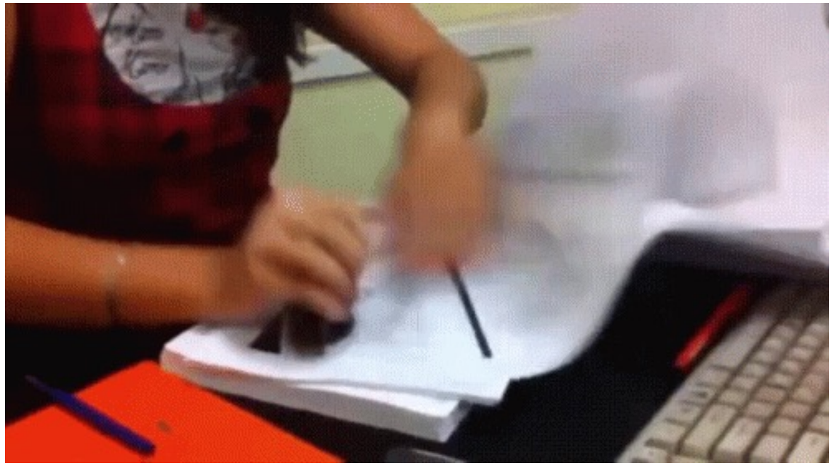
What Will Your Assessor Be Looking For?

NIST SP 800-171A Potential Assessment Methods and Objects

- **Examine**
  - The process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., specifications, mechanisms, activities).
    - [SELECT FROM: Identification and Authentication Policy; Procedures addressing user identification and authentication; etc.]
- **Interview**
  - The process of holding discussions with individuals or groups of individuals to facilitate understanding, achieve clarification, or obtain evidence.
    - [SELECT FROM: Personnel with system operations responsibilities, etc.]
- **Test**
  - The process of exercising assessment objects (i.e., activities, mechanisms under specified conditions to compare actual with expect behavior.
    - [SELECT FROM: Mechanisms supporting or implementing multifactor authentication capability]

Pay attention to the verbs

Associated with Documentation	Associated with Action
Identified	Limited
Defined	Implemented
Specified	Performed



3.1.22: Control CUI posted or processed on publicly accessible systems

- *Determine if:*
  - *[a] individuals authorized to post or process information on publicly accessible systems are identified.*
  - *[b] procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.*
  - *[c] a review process is in place prior to posting of any content to publicly accessible systems.*
  - *[d] mechanisms are in place to remove and address improper posting of CUI.*

3.1.22: Control CUI posted or processed on publicly accessible systems

- *Determine if:*
  - *[a] individuals authorized to post or process information on publicly accessible systems are identified.*
  - *[b] procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.*
  - *[c] a review process is in place prior to posting of any content to publicly accessible systems.*
  - *[d] mechanisms are in place to remove and address improper posting of CUI.*

3.1.22: Control CUI posted or processed on publicly accessible systems

- **_Discussion:_** *In accordance with laws, Executive Orders, directives, policies, regulations, or standards, the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, CUI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Individuals authorized to post CUI onto publicly accessible systems are designated. The content of information is reviewed prior to posting onto publicly accessible systems to ensure that nonpublic information is not included.*

3.1.22: Control CUI posted or processed on publicly accessible systems

- ***Discussion:*** *In accordance with laws, Executive Orders, directives, policies, regulations, or standards, the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, CUI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Individuals authorized to post CUI onto publicly accessible systems are designated. The content of information is reviewed prior to posting onto publicly accessible systems to ensure that nonpublic information is not included.*

[a] individuals authorized to post or process information on publicly accessible systems are identified

- *Potential solution:*
  - *Identify the individual*
    - *(e.g., John Smith)*
  - *Roles matrix*
    - *(e.g., HR Department)*

MARKETING
PAYROLL
IT
ENGINEER
HR
CEO
WHEN YOU DON'T HAVE ENOUGH EMPLOYEES TO SEPARATE DUTIES
imgflip.com

ROLES MATRIX

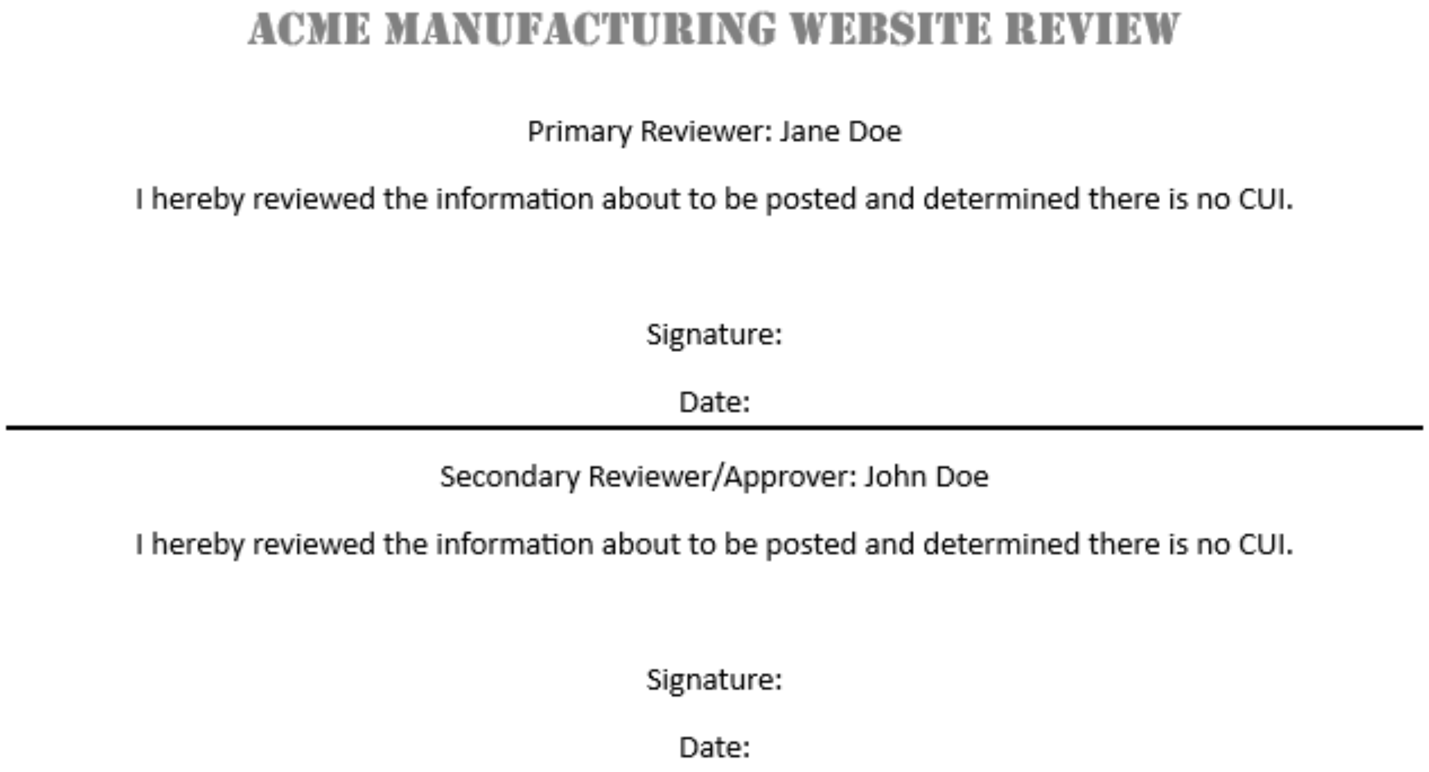
Role	Assigned To
HR	John Doe
Engineer	John Doe
IT	John Doe
Payroll	John Doe
Marketing	John Doe

3.1.22: Control CUI posted or processed on publicly accessible systems

- *Determine if:*
  - *[a] individuals authorized to post or process information on publicly accessible systems are identified.*
  - *[b] procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.*
  - *[c] a review process is in place prior to posting of any content to publicly accessible systems.*
  - *[d] mechanisms are in place to remove and address improper posting of CUI.*

(b) procedures to ensure CUI is not posted or processed on publicly accessible systems are identified

- *Potential solution:*
  - *Website Review Form*



ACME MANUFACTURING WEBSITE REVIEW

Primary Reviewer: Jane Doe

I hereby reviewed the information about to be posted and determined there is no CUI.

Signature:

Date:

Secondary Reviewer/Approver: John Doe

I hereby reviewed the information about to be posted and determined there is no CUI.

Signature:

Date:

3.1.22: Control CUI posted or processed on publicly accessible systems

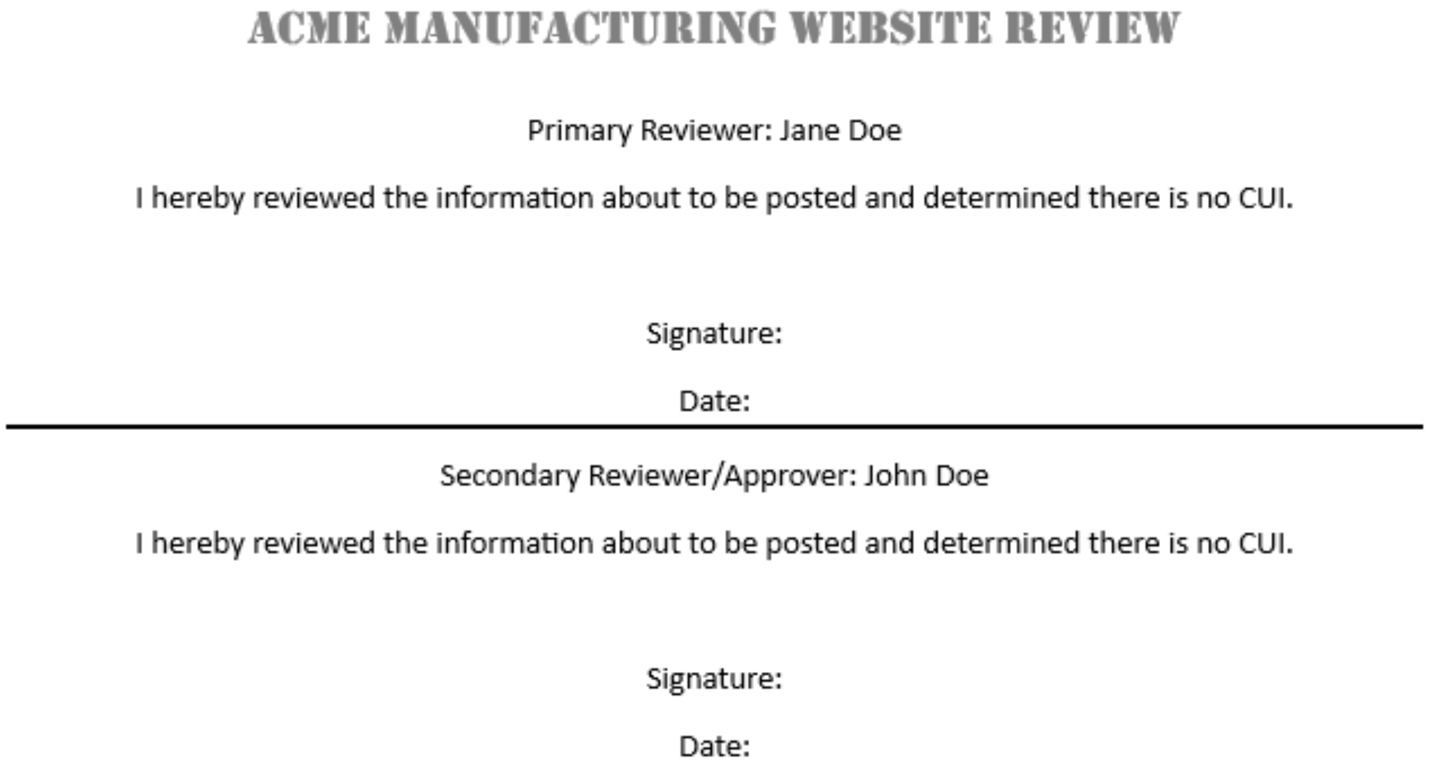
- *Determine if:*
  - *[a] individuals authorized to post or process information on publicly accessible systems are identified.*
  - *[b] procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.*
  - *[c] a review process is in place prior to posting of any content to publicly accessible systems.*
  - *[d] mechanisms are in place to remove and address improper posting of CUI.*

3.1.22: Control CUI posted or processed on publicly accessible systems

- ***Discussion:*** *In accordance with laws, Executive Orders, directives, policies, regulations, or standards, the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, CUI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Individuals authorized to post CUI onto publicly accessible systems are designated. The content of information is reviewed prior to posting onto publicly accessible systems to ensure that nonpublic information is not included.*

[c] a review process is in place prior to posting of any content to publicly accessible systems

- *Potential solution:*
  - *Website Review Form*



ACME MANUFACTURING WEBSITE REVIEW

Primary Reviewer: Jane Doe

I hereby reviewed the information about to be posted and determined there is no CUI.

Signature:

Date:

Secondary Reviewer/Approver: John Doe

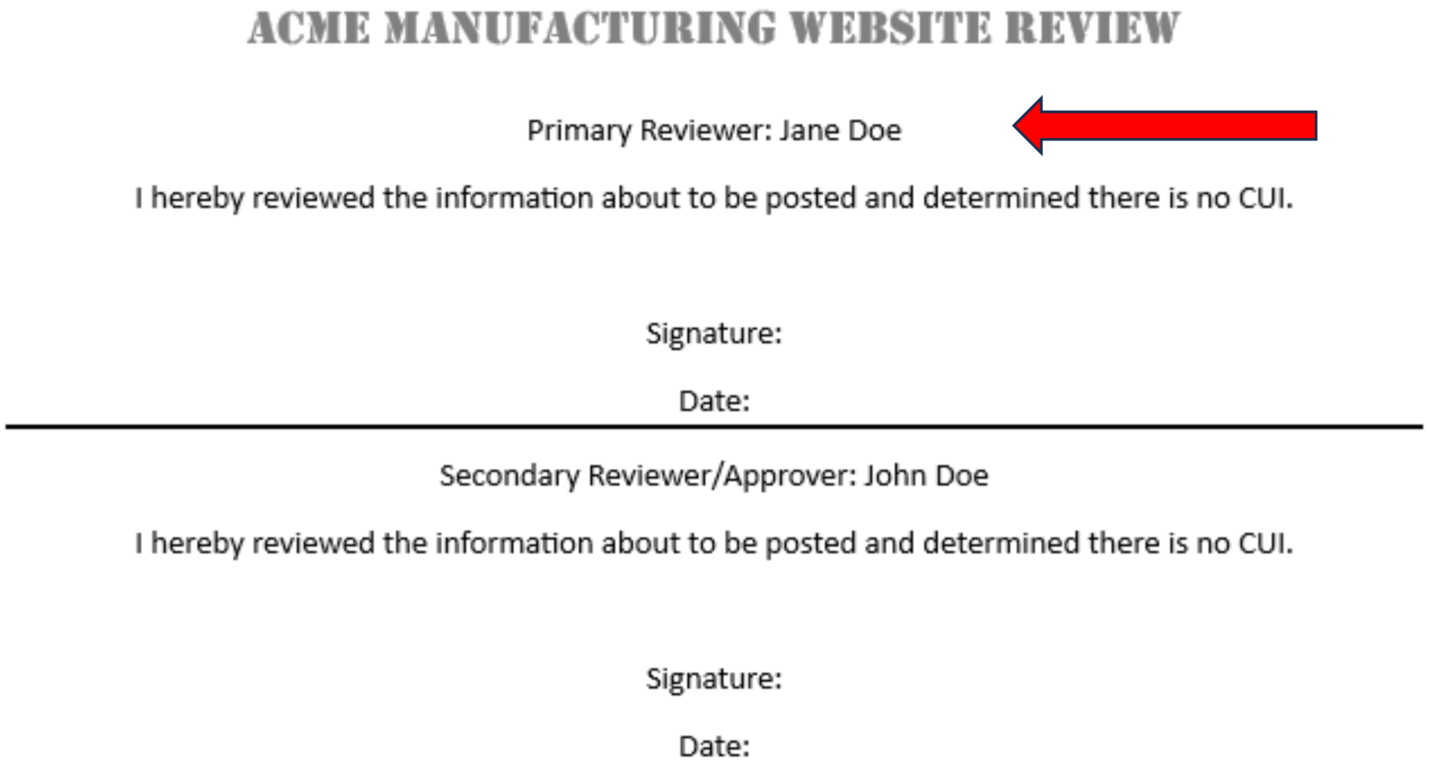
I hereby reviewed the information about to be posted and determined there is no CUI.

Signature:

Date:

[c] a review process is in place prior to posting of any content to publicly accessible systems

- *Potential solution:*
  - *Website Review Form*



ACME MANUFACTURING WEBSITE REVIEW

Primary Reviewer: Jane Doe

I hereby reviewed the information about to be posted and determined there is no CUI.

Signature:

Date:

Secondary Reviewer/Approver: John Doe

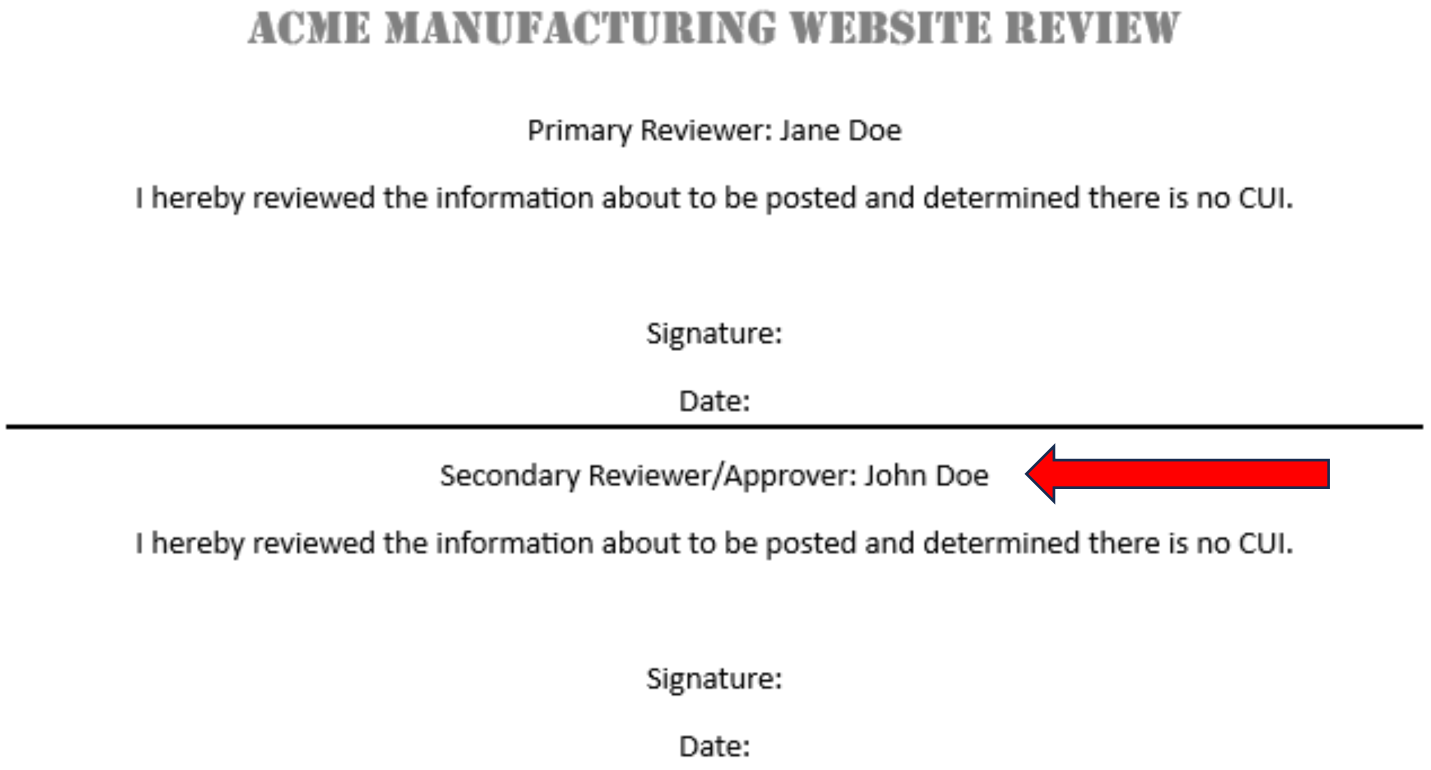
I hereby reviewed the information about to be posted and determined there is no CUI.

Signature:

Date:

[c] a review process is in place prior to posting of any content to publicly accessible systems

- *Potential solution:*
  - *Website Review Form*



ACME MANUFACTURING WEBSITE REVIEW

Primary Reviewer: Jane Doe

I hereby reviewed the information about to be posted and determined there is no CUI.

Signature:

Date:

Secondary Reviewer/Approver: John Doe

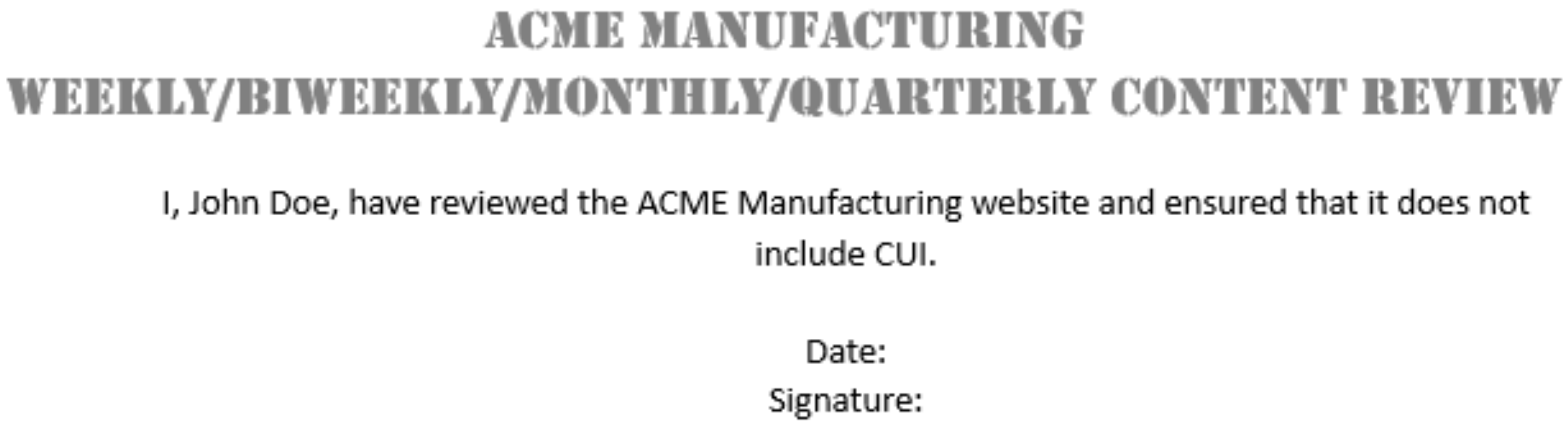
I hereby reviewed the information about to be posted and determined there is no CUI.

Signature:

Date:

[d] content on publicly accessible systems is reviewed to ensure that it does not include CUI

- *Potential Solution:*
  - *Weekly/Biweekly/Monthly/Quarterly Review*



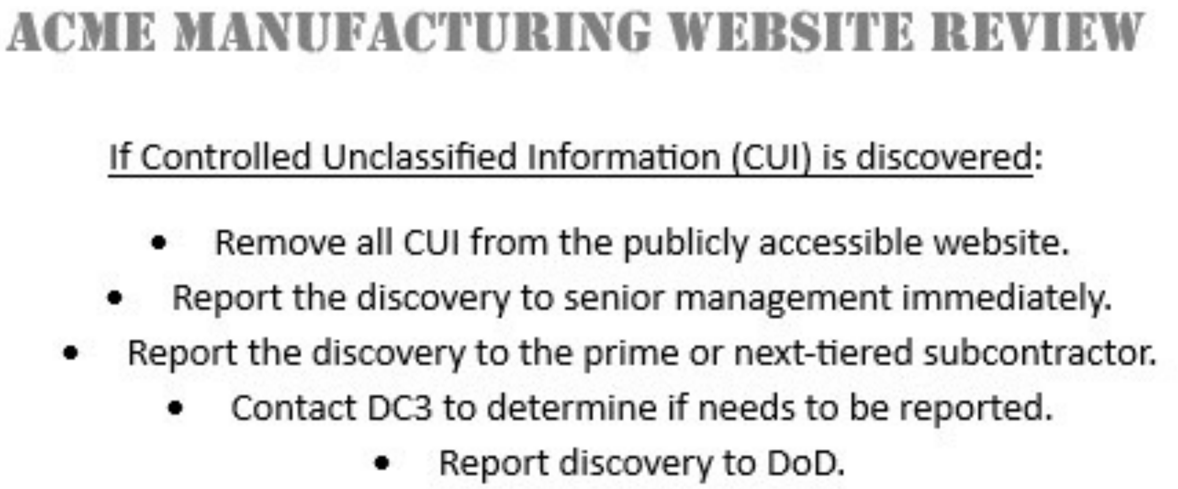
ACME MANUFACTURING
WEEKLY/BIWEEKLY/MONTHLY/QUARTERLY CONTENT REVIEW

I, John Doe, have reviewed the ACME Manufacturing website and ensured that it does not include CUI.

Date:
Signature:

[e] mechanisms are in place to remove and address improper posting of CUI

- *Potential solution:*
  - *Website Review Form*



ACME MANUFACTURING WEBSITE REVIEW

<u>If Controlled Unclassified Information (CUI) is discovered</u>:

- Remove all CUI from the publicly accessible website.
- Report the discovery to senior management immediately.
- Report the discovery to the prime or next-tiered subcontractor.
- Contact DC3 to determine if needs to be reported.
- Report discovery to DoD.

DFARS 252.204-7012
Paragraph [c] requirement

3.3.1: Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity

- *Determine if:*
  - *[a] audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.*
  - *[b] the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.*
  - *[c] audit records are created (generated).*
  - *[d] audit records, once created, contain the defined content.*
  - *[e] retention requirements for audit records are defined.*
  - *[f] audit records are retained as defined.*

3.3.1: Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity

- *Determine if:*
  - *[a] audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.*
  - *[b] the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.*
  - *[c] audit records are created (generated).*
  - *[d] audit records, once created, contain the defined content.*
  - *[e] retention requirements for audit records are defined.*
  - *[f] audit records are retained as defined.*

[a] audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.

- *Potential solution*:
  - *audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified. They include, but are not limited to, the following data connectors:*
    - *Microsoft Entra ID*
      - *Audit Logs*
      - *Sign In Logs*

Microsoft
Entra ID

3.3.1: Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity

- *Determine if:*
  - *[a] audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.*
  - *[b] the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.*
  - *[c] audit records are created (generated).*
  - *[d] audit records, once created, contain the defined content.*
  - *[e] retention requirements for audit records are defined.*
  - *[f] audit records are retained as defined.*

3.3.1: Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity

- ***<u>Discussion:</u>*** *An event is any observable occurrence in a system, which includes unlawful or unauthorized system activity. Organizations identify event types for which a logging functionality is needed as those events which are significant and relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing auditing needs. Event types can include password changes, failed logons or failed accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the monitoring and auditing appropriate for each of the CUI security requirements. Monitoring and auditing requirements can be balanced with other system needs. For example, organizations may determine that systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance.*

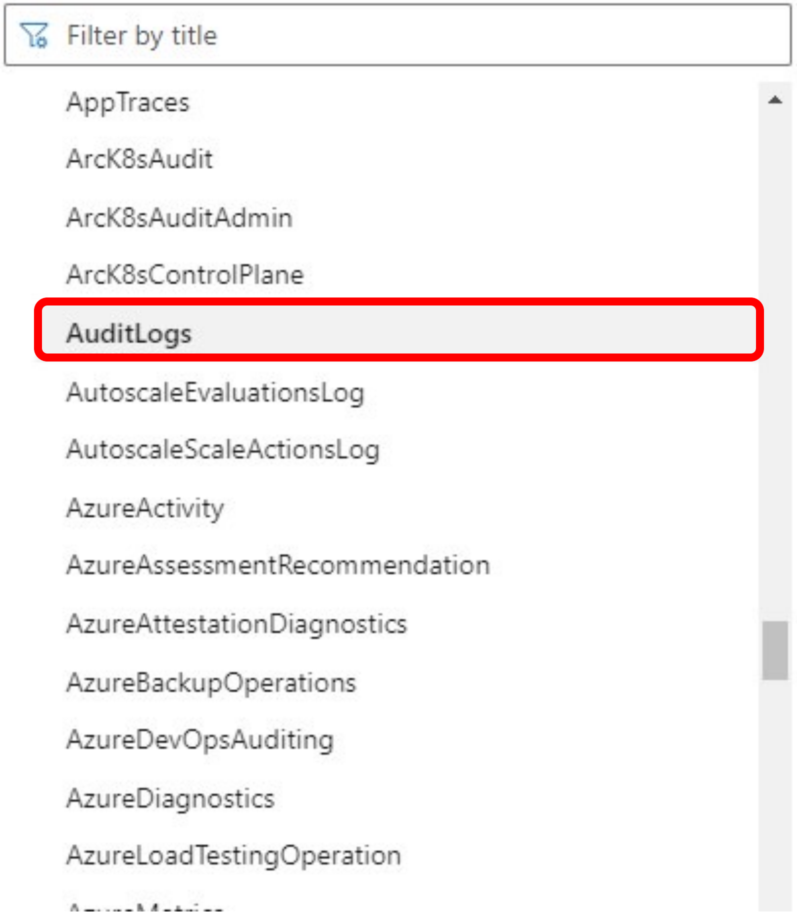
- *Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit logging capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of event types, the logging necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented or cloud-based architectures.*

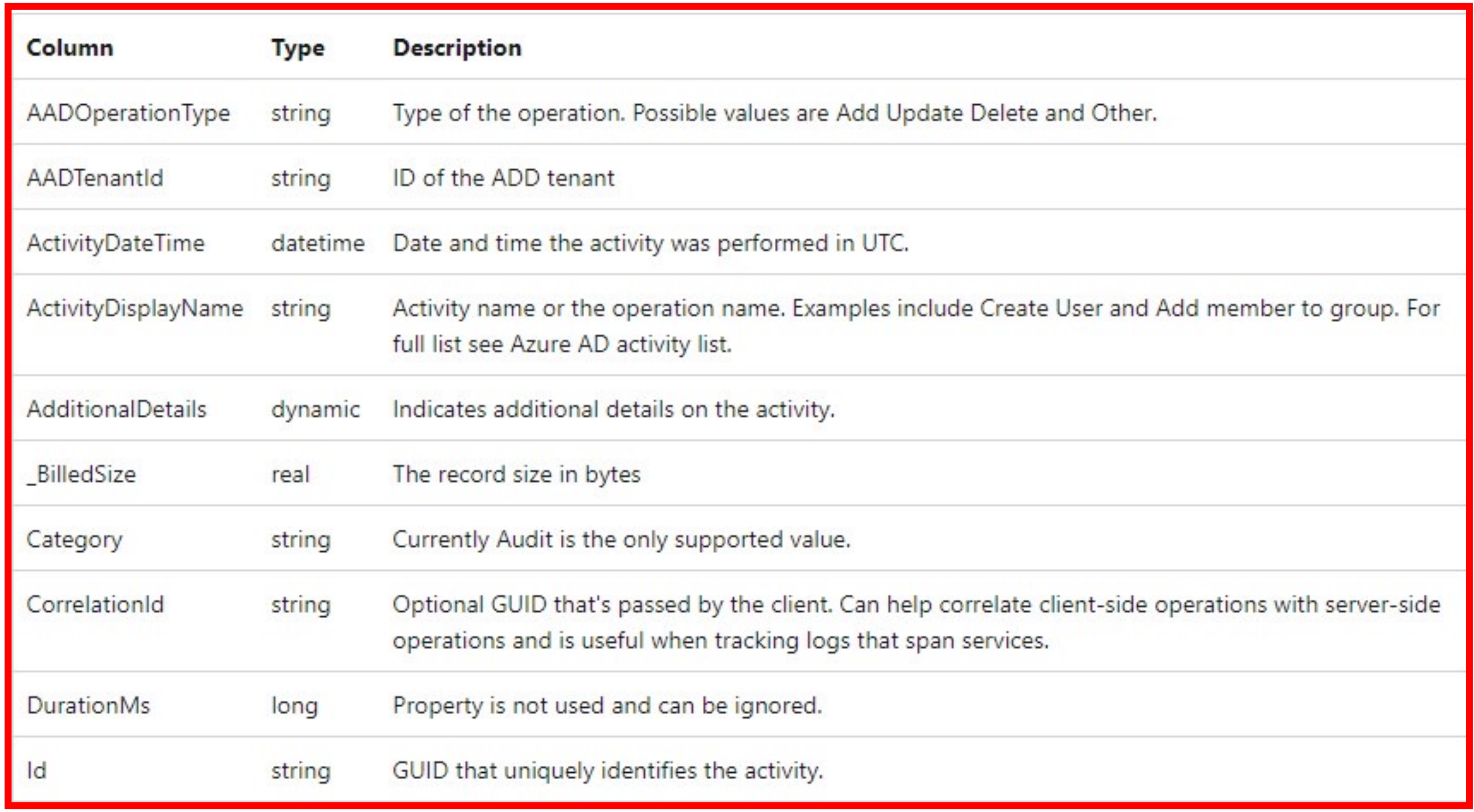
- *Audit record content that may be necessary to satisfy this requirement includes time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the system after the event occurred).*

- *Detailed information that organizations may consider in audit records includes full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit log information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest. Audit logs are reviewed and analyzed as often as needed to provide important information to organizations to facilitate risk-based decision making.*

- *[SP 800-92] provides guidance on security log management.*

[b] the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined





Column	Type	Description
AADOperationType	string	Type of the operation. Possible values are Add Update Delete and Other.
AADTenantId	string	ID of the ADD tenant
ActivityDateTime	datetime	Date and time the activity was performed in UTC.
ActivityDisplayName	string	Activity name or the operation name. Examples include Create User and Add member to group. For full list see Azure AD activity list.
AdditionalDetails	dynamic	Indicates additional details on the activity.
_BilledSize	real	The record size in bytes
Category	string	Currently Audit is the only supported value.
CorrelationId	string	Optional GUID that's passed by the client. Can help correlate client-side operations with server-side operations and is useful when tracking logs that span services.
DurationMs	long	Property is not used and can be ignored.
Id	string	GUID that uniquely identifies the activity.

3.3.1: Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity

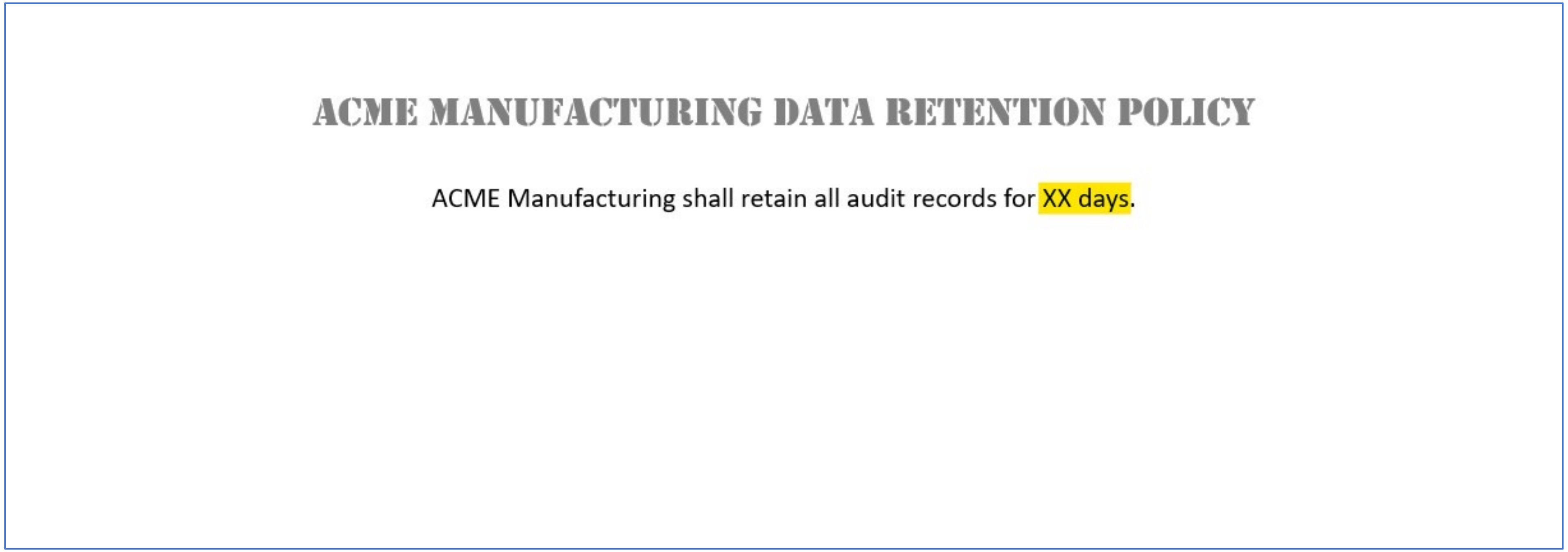
- *Determine if:*
  - *[a] audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.*
  - *[b] the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.*
  - *[c] audit records are created (generated).*
  - *[d] audit records, once created, contain the defined content.*
  - *[e] retention requirements for audit records are defined.*
  - *[f] audit records are retained as defined.*

3.3.1: Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity

- *Determine if:*
  - *[a] audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.*
  - *[b] the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.*
  - *[c] audit records are created (generated).*
  - *[d] audit records, once created, contain the defined content.*
  - *[e] retention requirements for audit records are defined.*
  - *[f] audit records are retained as defined.*

[e] retention requirements for audit records are defined

- *Potential solution:*
  - *Organizational Policy*

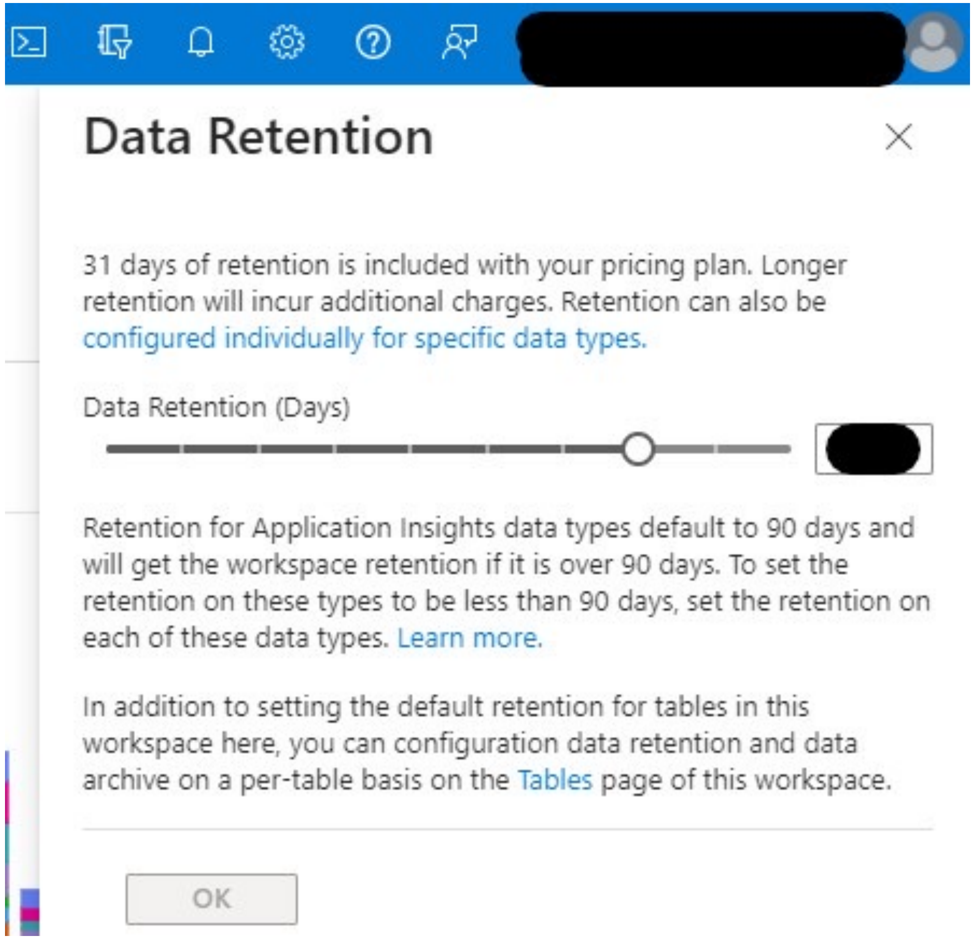


ACME MANUFACTURING DATA RETENTION POLICY

ACME Manufacturing shall retain all audit records for XX days.

[f] audit records are retained as specified

- *Potential solution:*
  - *Technical implementation*



[redacted]

Data Retention

31 days of retention is included with your pricing plan. Longer retention will incur additional charges. Retention can also be configured individually for specific data types.

Data Retention (Days) [redacted]

Retention for Application Insights data types default to 90 days and will get the workspace retention if it is over 90 days. To set the retention on these types to be less than 90 days, set the retention on each of these data types. Learn more.

In addition to setting the default retention for tables in this workspace here, you can configuration data retention and data archive on a per-table basis on the Tables page of this workspace.

3.3.3: Review and update audited events

- *Determine if:*
    - *[a] a process for determining when to review logged events is defined.*
    - *[b] event types being logged are reviewed in accordance with the defined review process.*
    - *[c] event types being logged are updated based on the review.*

3.3.3: Review and update audited events

- *Determine if:*
  - *[a] a process for determining when to review logged events is defined.*
  - *[b] event types being logged are reviewed in accordance with the defined review process.*
  - *[c] event types being logged are updated based on the review.*

3.3.3: Review and update audited events

- ***Discussion**: The intent of this requirement is to periodically re-evaluate which logged events will continue to be included in the list of events to be logged. The event types that are logged by organizations may change over time. Reviewing and updating the set of logged event types periodically is necessary to ensure that the current set remains necessary and sufficient.*

3.3.3: Review and update audited events

- ***Discussion***: *The intent of this requirement is to periodically re-evaluate which logged events will continue to be included in the list of events to be logged. The event types that are logged by organizations may change over time. Reviewing and updating the set of logged event types periodically is necessary to ensure that the current set remains necessary and sufficient.*

CMMC Glossary

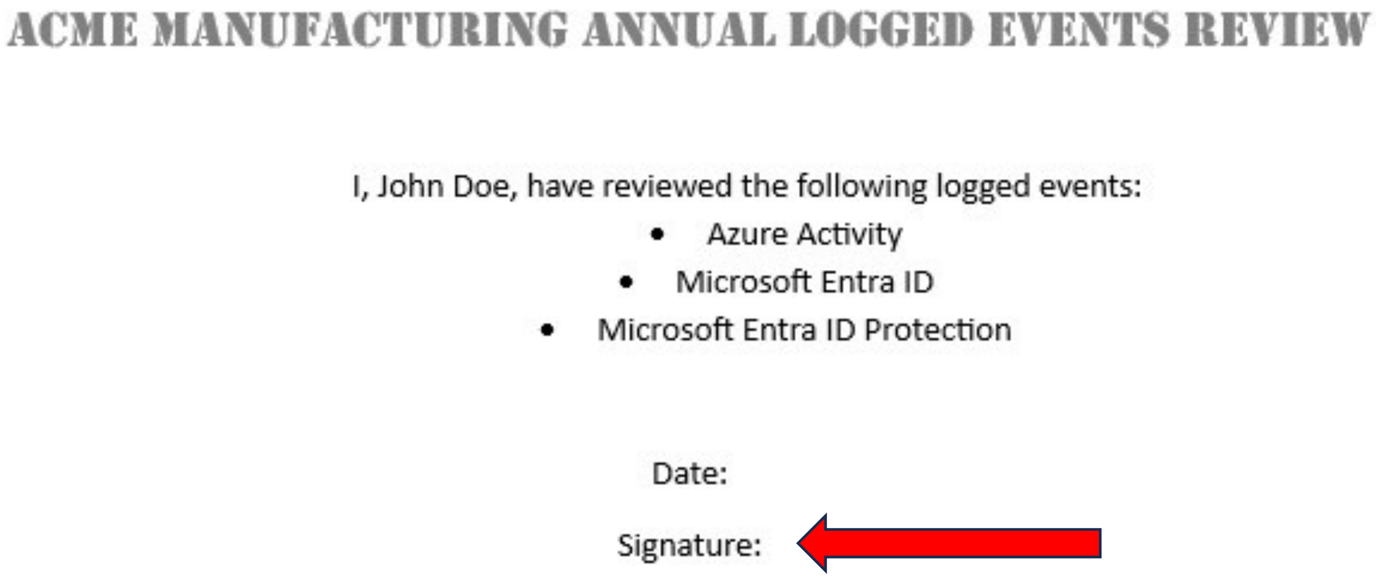
- *Occurring at regular intervals. As used in many practices within CMMC, the interval length is organizationally defined to provided contractor flexibility, with an interval length of no more than one year.*

CMMC Glossary

- *Occurring at regular intervals. As used in many practices within CMMC, the interval length is organizationally defined to provided contractor flexibility, with an interval length of no more than one year.*

[a] a process for determining when to review logged events is defined
[b] event types being logged are reviewed in accordance with the defined review process

- *Potential solution:*
  - *Organizational procedure*



ACME MANUFACTURING ANNUAL LOGGED EVENTS REVIEW

I, John Doe, have reviewed the following logged events:

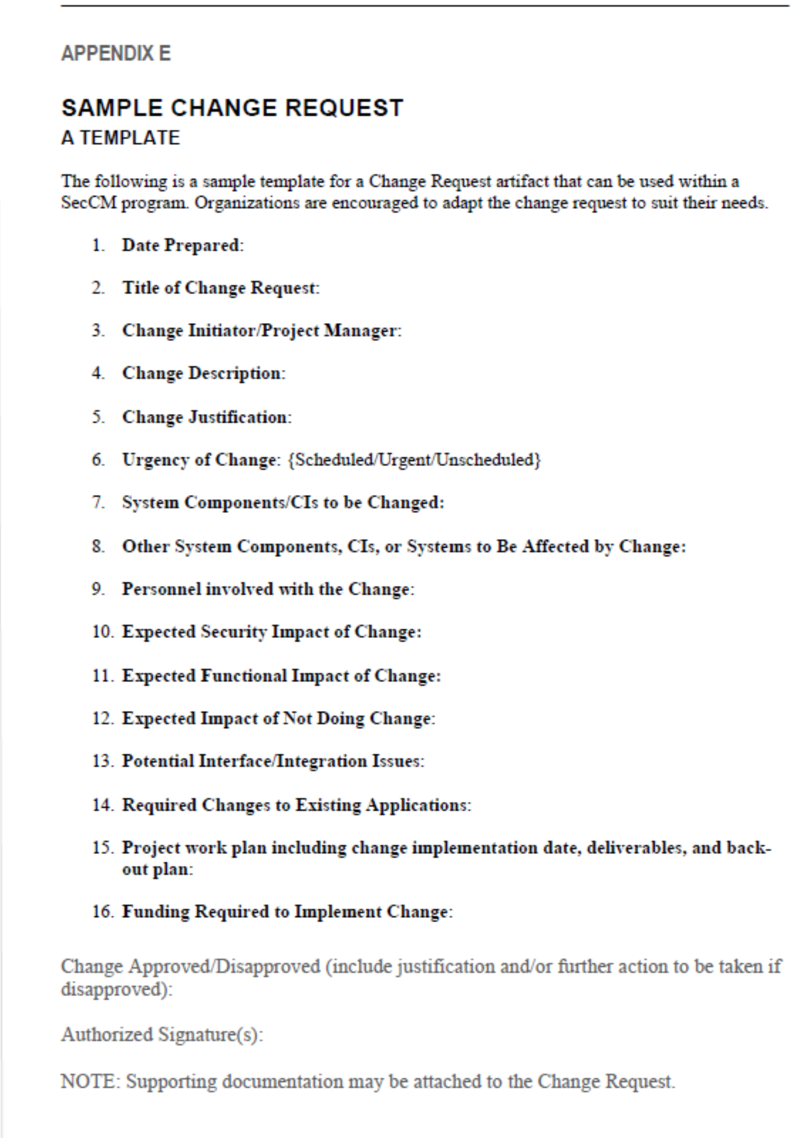
- Azure Activity
- Microsoft Entra ID
- Microsoft Entra ID Protection

Date:

Signature:

[c] event types being logged are updated based on the review based on the review

- *Potential Solution:*
  - *Configuration Change Management*
  - *Sample Change Request*
    - *NIST SP 800-128*



APPENDIX E

SAMPLE CHANGE REQUEST

A TEMPLATE

The following is a sample template for a Change Request artifact that can be used within a SecCM program. Organizations are encouraged to adapt the change request to suit their needs.

1. **Date Prepared**:
2. **Title of Change Request**:
3. **Change Initiator/Project Manager**:
4. **Change Description**:
5. **Change Justification**:
6. **Urgency of Change**: {Scheduled/Urgent/Unscheduled}
7. **System Components/CIs to be Changed:**
8. **Other System Components, CIs, or Systems to Be Affected by Change:**
9. **Personnel involved with the Change**:
10. **Expected Security Impact of Change:**
11. **Expected Functional Impact of Change:**
12. **Expected Impact of Not Doing Change**:
13. **Potential Interface/Integration Issues**:
14. **Required Changes to Existing Applications**:
15. **Project work plan including change implementation date, deliverables, and back-out plan**:
16. **Funding Required to Implement Change**:

Change Approved/Disapproved (include justification and/or further action to be taken if disapproved):

Authorized Signature(s):

NOTE: Supporting documentation may be attached to the Change Request.

3.4.3: Track, review, approve or disapprove, and log changes to organizational systems

- *Determine if:*
  - *[a] changes to the system are tracked.*
  - *[b] changes to the system are reviewed.*
  - *[c] changes to the system are approved or disapproved.*
  - *[d] changes to the system are logged.*

3.4.3: Track, review, approve or disapprove, and log changes to organizational systems

- ***Discussion**: Tracking, reviewing, approving/disapproving, and logging changes is called configuration change control. Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled and unauthorized changes, and changes to remediate vulnerabilities.*
- *Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes to systems. For new development systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards or Change Advisory Boards. Audit logs of changes include activities before and after changes are made to organizational systems and the activities required to implement such changes.*
- *[SP 800-128] provides guidance on configuration change control.*

3.4.3: Track, review, approve or disapprove, and log changes to organizational systems

- ***Discussion****: Tracking, reviewing, approving/disapproving, and logging changes is called configuration change control. Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled and unauthorized changes, and changes to remediate vulnerabilities.*
- *Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes to systems. For new development systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards or Change Advisory Boards. Audit logs of changes include activities before and after changes are made to organizational systems and the activities required to implement such changes.*
- *[SP 800-128] provides guidance on configuration change control.*

3.4.3: Track, review, approve or disapprove, and log changes to organizational systems

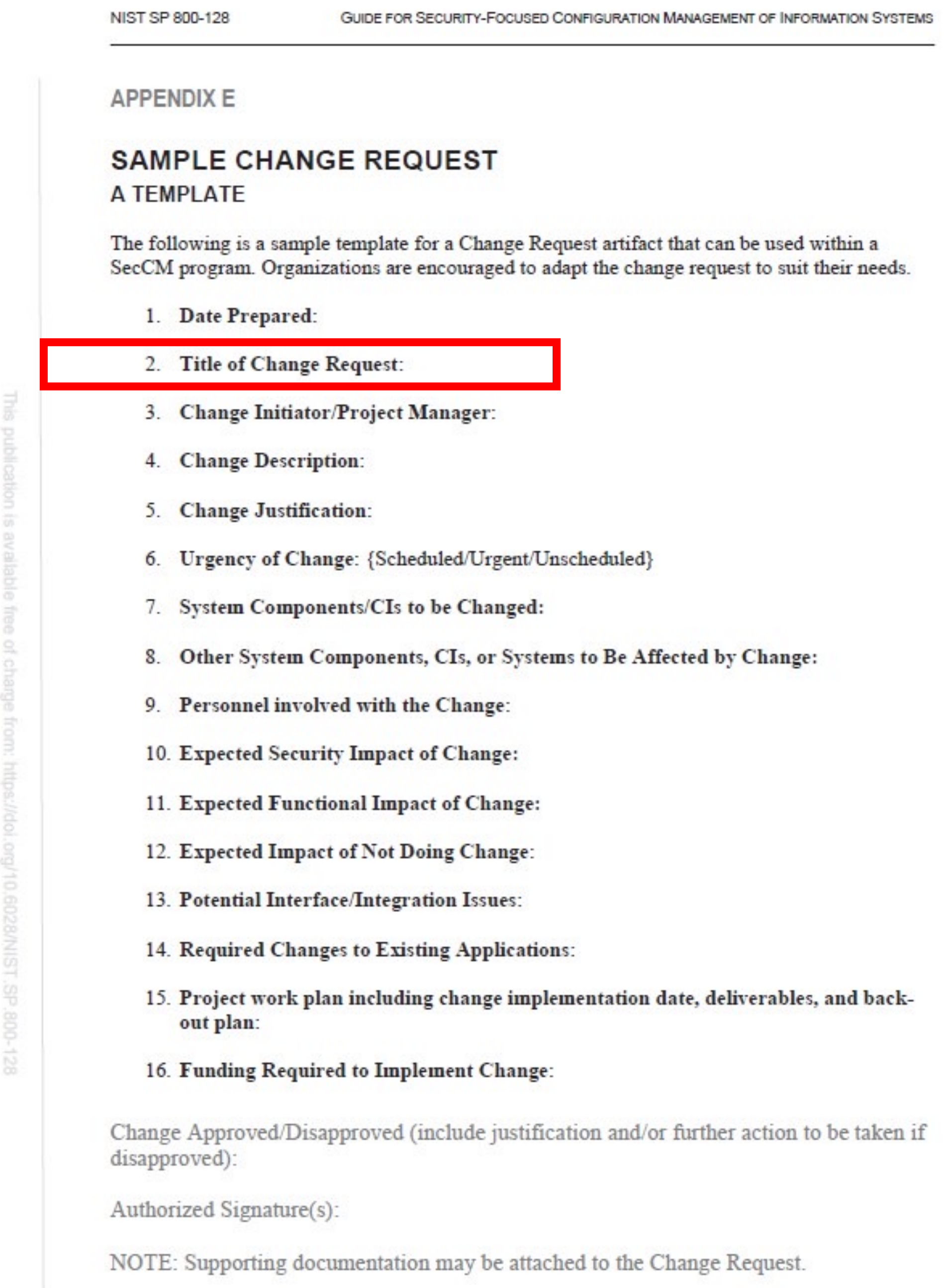
- ***Discussion***: *Tracking, reviewing, approving/disapproving, and logging changes is called configuration change control. Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled and unauthorized changes, and changes to remediate vulnerabilities.*
- *Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes to systems. For new development systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards or Change Advisory Boards. Audit logs of changes include activities before and after changes are made to organizational systems and the activities required to implement such changes.*
- *[SP 800-128] provides guidance on configuration change control.*

[a] changes to the system are tracked

[b] changes to the system are reviewed

[c] changes to the system are approved or disapproved

[d] changes to the system are logged



APPENDIX E

SAMPLE CHANGE REQUEST

A TEMPLATE

The following is a sample template for a Change Request artifact that can be used within a SecCM program. Organizations are encouraged to adapt the change request to suit their needs.

1. **Date Prepared**:
2. **Title of Change Request**:
3. **Change Initiator/Project Manager**:
4. **Change Description**:
5. **Change Justification**:
6. **Urgency of Change**: {Scheduled/Urgent/Unscheduled}
7. **System Components/CIs to be Changed:**
8. **Other System Components, CIs, or Systems to Be Affected by Change:**
9. **Personnel involved with the Change**:
10. **Expected Security Impact of Change:**
11. **Expected Functional Impact of Change:**
12. **Expected Impact of Not Doing Change**:
13. **Potential Interface/Integration Issues**:
14. **Required Changes to Existing Applications**:
15. **Project work plan including change implementation date, deliverables, and back-out plan**:
16. **Funding Required to Implement Change**:

Change Approved/Disapproved (include justification and/or further action to be taken if disapproved):

Authorized Signature(s):

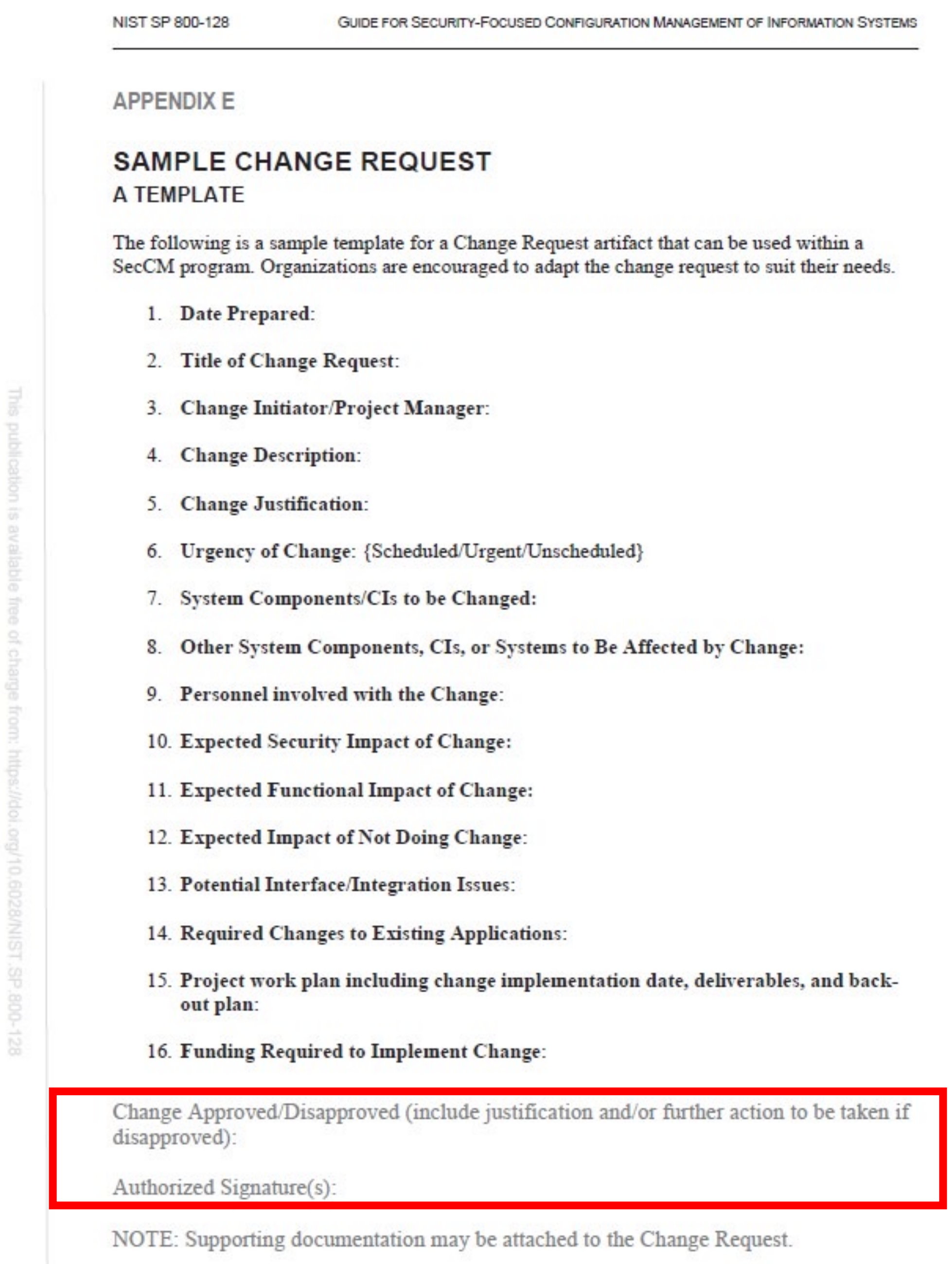
NOTE: Supporting documentation may be attached to the Change Request.

[a] changes to the system are tracked

[b] changes to the system are reviewed

[c] changes to the system are approved or disapproved

[d] changes to the system are logged



APPENDIX E

SAMPLE CHANGE REQUEST

A TEMPLATE

The following is a sample template for a Change Request artifact that can be used within a SecCM program. Organizations are encouraged to adapt the change request to suit their needs.

1. **Date Prepared**:
2. **Title of Change Request**:
3. **Change Initiator/Project Manager**:
4. **Change Description**:
5. **Change Justification**:
6. **Urgency of Change**: {Scheduled/Urgent/Unscheduled}
7. **System Components/CIs to be Changed:**
8. **Other System Components, CIs, or Systems to Be Affected by Change:**
9. **Personnel involved with the Change**:
10. **Expected Security Impact of Change:**
11. **Expected Functional Impact of Change:**
12. **Expected Impact of Not Doing Change**:
13. **Potential Interface/Integration Issues**:
14. **Required Changes to Existing Applications**:
15. **Project work plan including change implementation date, deliverables, and back-out plan**:
16. **Funding Required to Implement Change**:

Change Approved/Disapproved (include justification and/or further action to be taken if disapproved):

Authorized Signature(s):

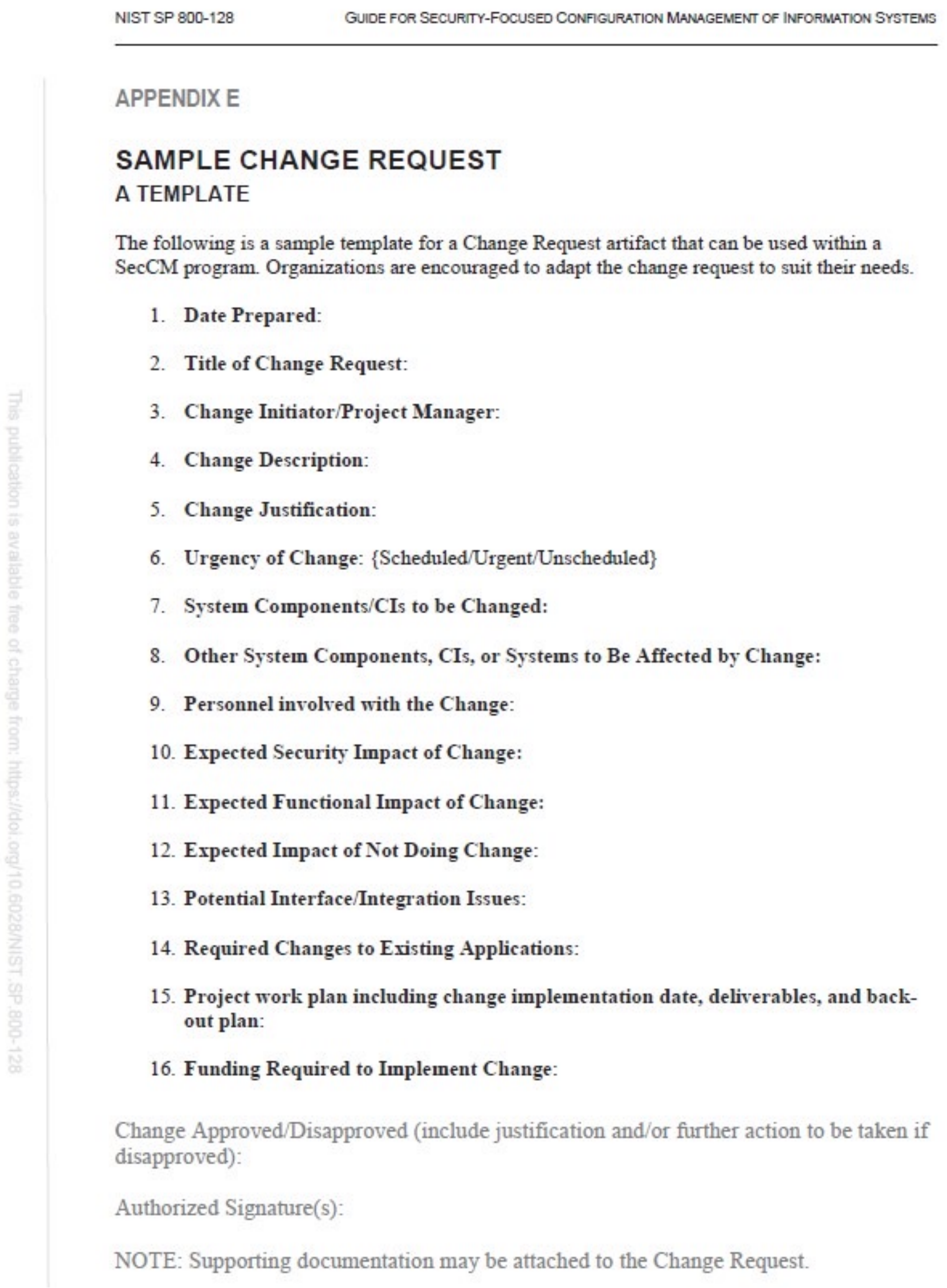
NOTE: Supporting documentation may be attached to the Change Request.

[a] changes to the system are tracked

[b] changes to the system are reviewed

[c] changes to the system are approved or disapproved

[d] changes to the system are logged



APPENDIX E

SAMPLE CHANGE REQUEST

A TEMPLATE

The following is a sample template for a Change Request artifact that can be used within a SecCM program. Organizations are encouraged to adapt the change request to suit their needs.

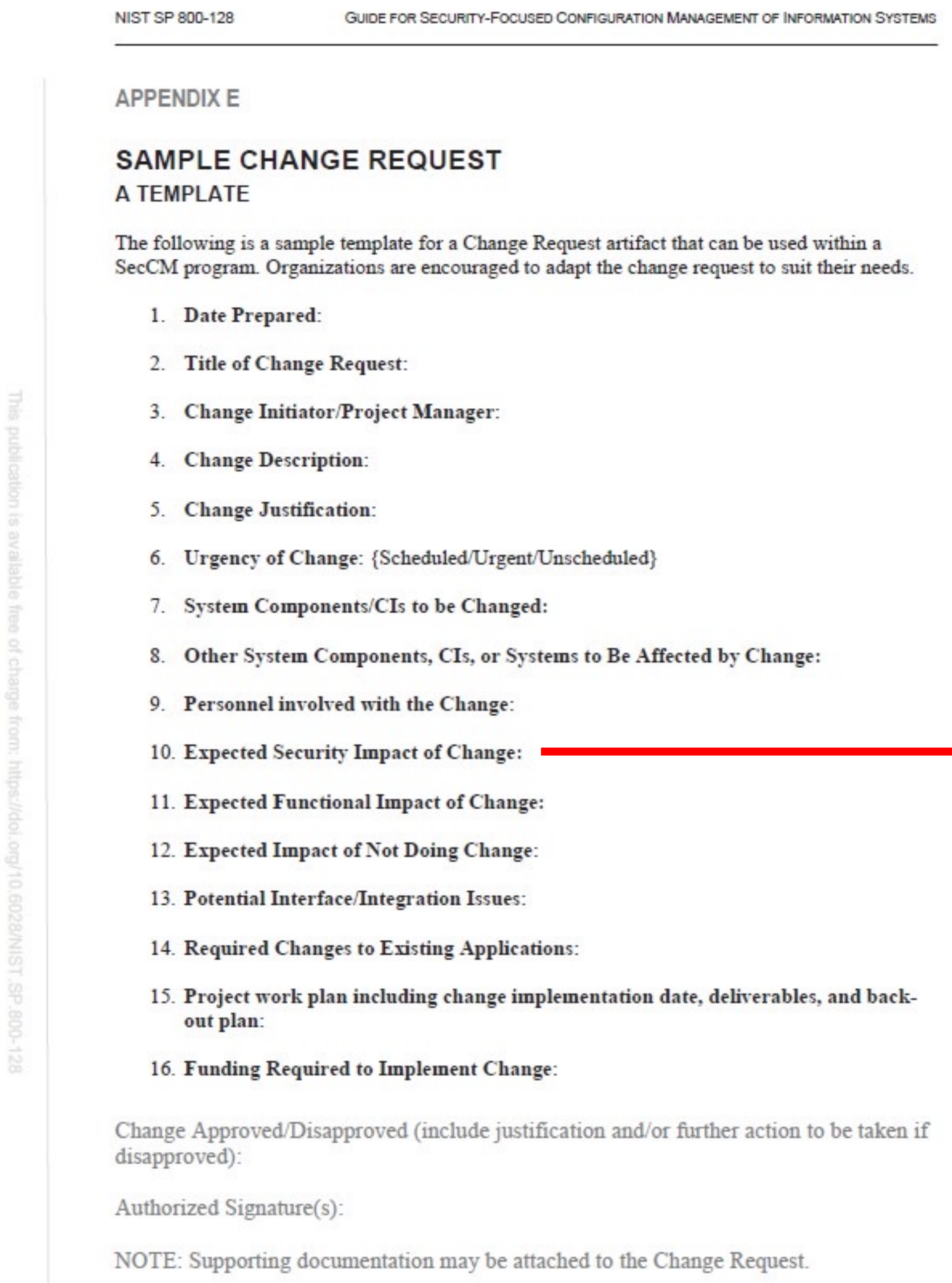
1. **Date Prepared**:
2. **Title of Change Request**:
3. **Change Initiator/Project Manager**:
4. **Change Description**:
5. **Change Justification**:
6. **Urgency of Change**: {Scheduled/Urgent/Unscheduled}
7. **System Components/CIs to be Changed:**
8. **Other System Components, CIs, or Systems to Be Affected by Change:**
9. **Personnel involved with the Change**:
10. **Expected Security Impact of Change:**
11. **Expected Functional Impact of Change:**
12. **Expected Impact of Not Doing Change**:
13. **Potential Interface/Integration Issues**:
14. **Required Changes to Existing Applications**:
15. **Project work plan including change implementation date, deliverables, and back-out plan**:
16. **Funding Required to Implement Change**:

Change Approved/Disapproved (include justification and/or further action to be taken if disapproved):

Authorized Signature(s):

NOTE: Supporting documentation may be attached to the Change Request.

[a] changes to the system are tracked
[b] changes to the system are reviewed
[c] changes to the system are approved or disapproved
[d] changes to the system are logged



APPENDIX E

SAMPLE CHANGE REQUEST

A TEMPLATE

The following is a sample template for a Change Request artifact that can be used within a SecCM program. Organizations are encouraged to adapt the change request to suit their needs.

1. **Date Prepared**:
2. **Title of Change Request**:
3. **Change Initiator/Project Manager**:
4. **Change Description**:
5. **Change Justification**:
6. **Urgency of Change**: {Scheduled/Urgent/Unscheduled}
7. **System Components/CIs to be Changed:**
8. **Other System Components, CIs, or Systems to Be Affected by Change:**
9. **Personnel involved with the Change**:
10. **Expected Security Impact of Change**:
11. **Expected Functional Impact of Change:**
12. **Expected Impact of Not Doing Change**:
13. **Potential Interface/Integration Issues**:
14. **Required Changes to Existing Applications**:
15. **Project work plan including change implementation date, deliverables, and back-out plan**:
16. **Funding Required to Implement Change**:

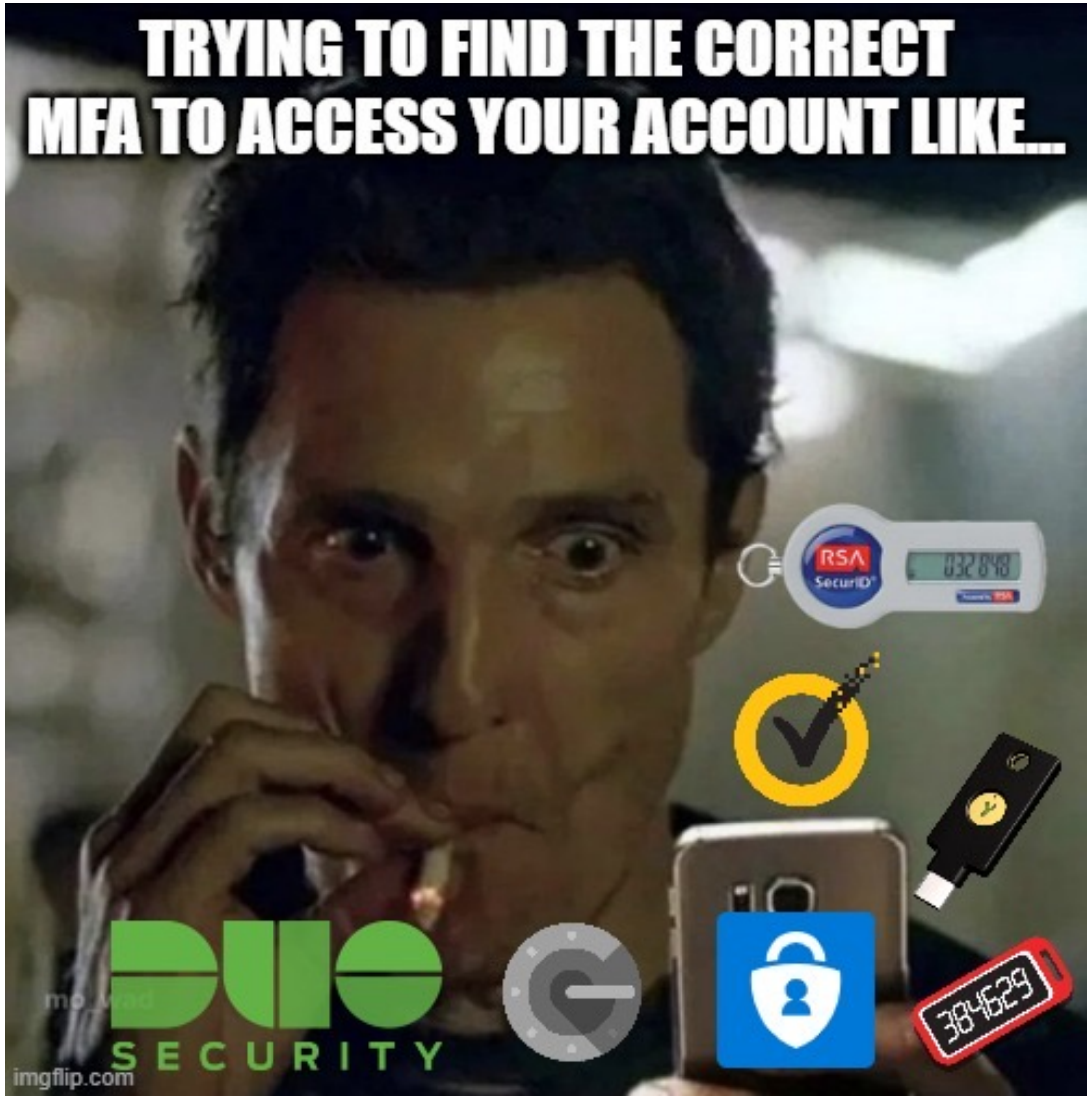
Change Approved/Disapproved (include justification and/or further action to be taken if disapproved):

Authorized Signature(s):

NOTE: Supporting documentation may be attached to the Change Request.

Can be used to satisfy ***3.4.4: Analyze the security impact of changes prior to implementation***

3.5.3: Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts


TRYING TO FIND THE CORRECT MFA TO ACCESS YOUR ACCOUNT LIKE...
RSA SecurID
032848
DUO SECURITY
384629
imgflip.com

3.5.3: Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts

- *Determine if:*
  - *[a] privileged accounts are identified.*
  - *[b] multifactor authentication is implemented for local access to privileged accounts.*
  - *[c] multifactor authentication is implemented for network access to privileged accounts.*
  - *[d] multifactor authentication is implemented for network access to non-privileged accounts.*

3.5.3: Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts

- *Determine if:*
  - *[a] privileged accounts are identified.*
  - *[b] multifactor authentication is implemented for local access to privileged accounts.*
  - *[c] multifactor authentication is implemented for network access to privileged accounts.*
  - *[d] multifactor authentication is implemented for network access to non-privileged accounts.*

[a] Privileged accounts are identified

NIST SP 800-171 Glossary

- *Privileged Account*
  - *A system account with authorizations of a privileged user*
- *Privileged User*
  - *A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform*

[a] Privileged accounts are identified

NIST SP 800-171 Glossary

- *Privileged Account*
  - *A system account with authorizations of a privileged user*
- *Privileged User*
  - *A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform*

NIST SPECIAL PUBLICATION
SP 800-171
171
REVISION 2
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

[a] Privileged accounts are identified

- *Examples of privileged accounts:*
  - *Firewall administrator accounts*
  - *Local administrator accounts*
  - *Domain administrator accounts*

WatchGuard®

CISCO

FORTINET®

CISCO

Cisco Umbrella

SOPHOS

[a] Privileged accounts are identified

- *Solutions to identify privileged accounts:*
  - *Employee Onboarding Checklist*
  - *Privileged User Form*

3.1.1: Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems)

3.5.3: Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts

- *Determine if:*
  - *[a] privileged accounts are identified.*
  - *[b] multifactor authentication is implemented for local access to privileged accounts.*
  - *[c] multifactor authentication is implemented for network access to privileged accounts.*
  - *[d] multifactor authentication is implemented for network access to non-privileged accounts.*

[b] Multifactor authentication is implemented for local access to privileged accounts

- ***Discussion**: Access to organizational systems is defined as local access or network access. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. The use of encrypted virtual private networks for connections between organization-controlled and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information.*

[b] Multifactor authentication is implemented for local access to privileged accounts

- ***Discussion***: *Access to organizational systems is defined as local access or network access. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. The use of encrypted virtual private networks for connections between organization-controlled and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information.*

[b] Multifactor authentication is implemented for local access to privileged accounts

Something you have (e.g., one-time password (OTP) generating device like a fob, smart-card, or a mobile app on a smart phone

Something you know (e.g., password, passphrase, PIN)

Something you are (e.g., a biometric like a fingerprint or iris)

[b] Multifactor authentication is implemented for local access to privileged accounts

- ***Discussion***: *Access to organizational systems is defined as local access or network access. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. The use of encrypted virtual private networks for connections between organization-controlled and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information.*

[b] Multifactor authentication is implemented for local access to privileged accounts

DoD Procurement Toolbox

- *Q80: Security Requirement 3.5.3 – Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. What is meant by "multifactor authentication"?*
- *"For a PRIVILEGED user, even local access (e.g., to the standalone) requires MFA."*

(b) Multifactor authentication is implemented for local access to privileged accounts

DoD Procurement Toolbox

- *Q80: Security Requirement 3.5.3 – Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. What is meant by "multifactor authentication"?*
- *"For a PRIVILEGED user, even local access (e.g., to the standalone) requires MFA."*

3.5.3: Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts

- *Determine if:*
  - *[a] privileged accounts are identified.*
  - *[b] multifactor authentication is implemented for local access to privileged accounts.*
  - *[c] multifactor authentication is implemented for network access to privileged accounts.*
  - *[d] multifactor authentication is implemented for network access to non-privileged accounts.*

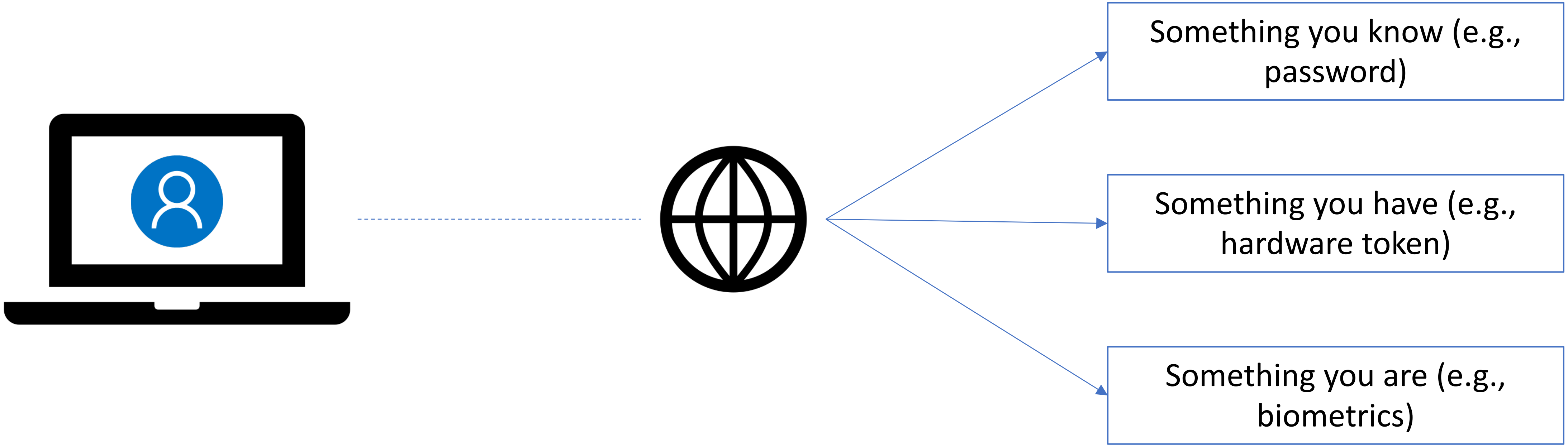
[c] Multifactor authentication is implemented for network access to privileged accounts

[d] Multifactor authentication is implemented for network access to non-privileged accounts

- ***Discussion**: Access to organizational systems is defined as local access or network access. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. The use of encrypted virtual private networks for connections between organization-controlled and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information.*

[c] Multifactor authentication is implemented for network access to privileged accounts

[d] Multifactor authentication is implemented for network access to non-privileged accounts



Something you know (e.g., password)

Something you have (e.g., hardware token)

Something you are (e.g., biometrics)

[c] Multifactor authentication is implemented for network access to privileged accounts

[d] Multifactor authentication is implemented for network access to non-privileged accounts

Microsoft
Office 365
Google
aws

3.7.3: Ensure equipment removed for off-site maintenance is sanitized of any CUI

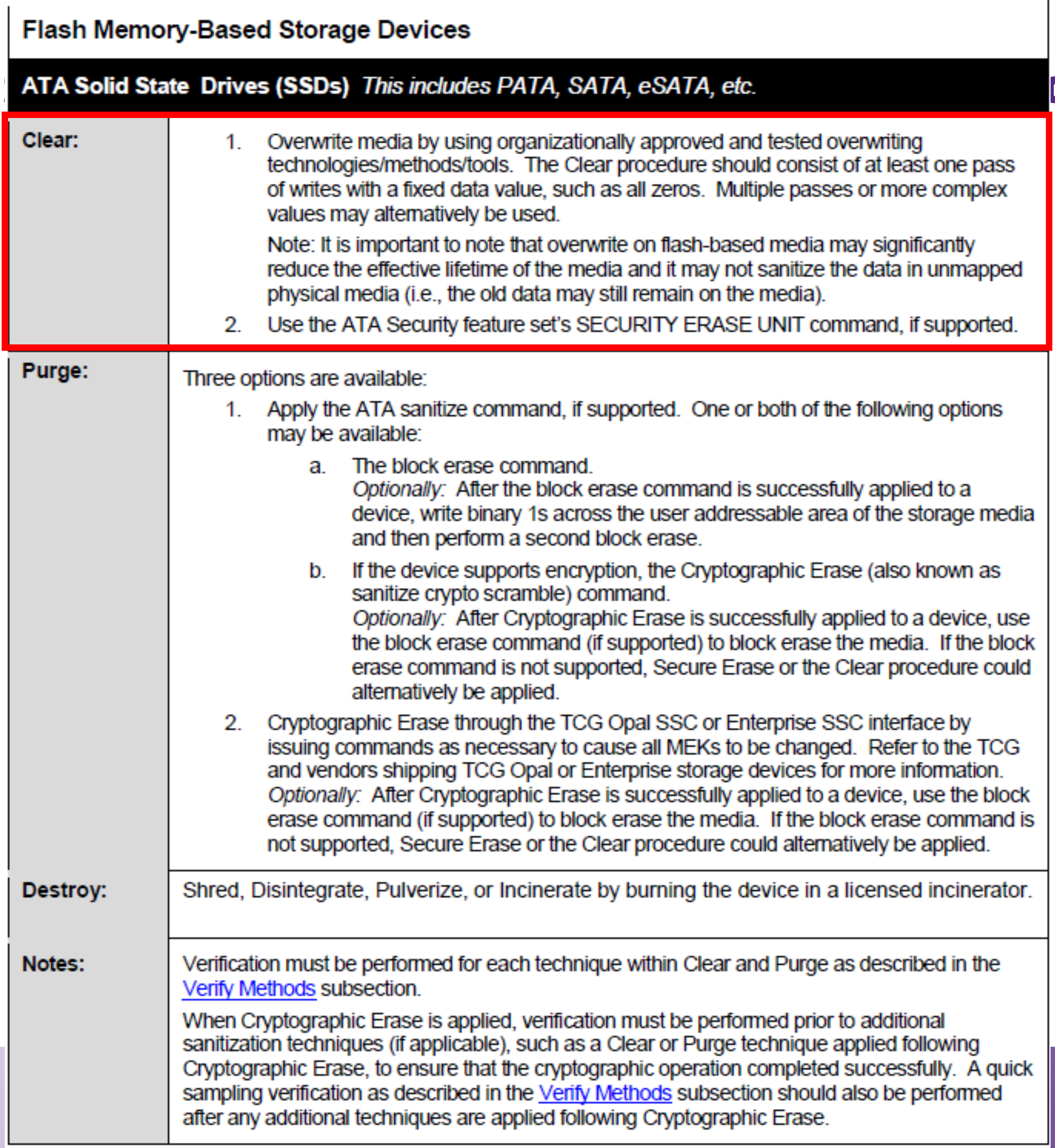
- *Determine if:*
  - *Equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI.*

3.7.3: Ensure equipment removed for off-site maintenance is sanitized of any CUI

- ***Discussion:*** *This requirement addresses the information security aspects of system maintenance that are performed off-site and applies to all types of maintenance to any system component (including applications) conducted by a local or nonlocal entity (e.g., in-contract, warranty, in- house, software maintenance agreement).*
- *[SP 800-88] provides guidance on media sanitization.*

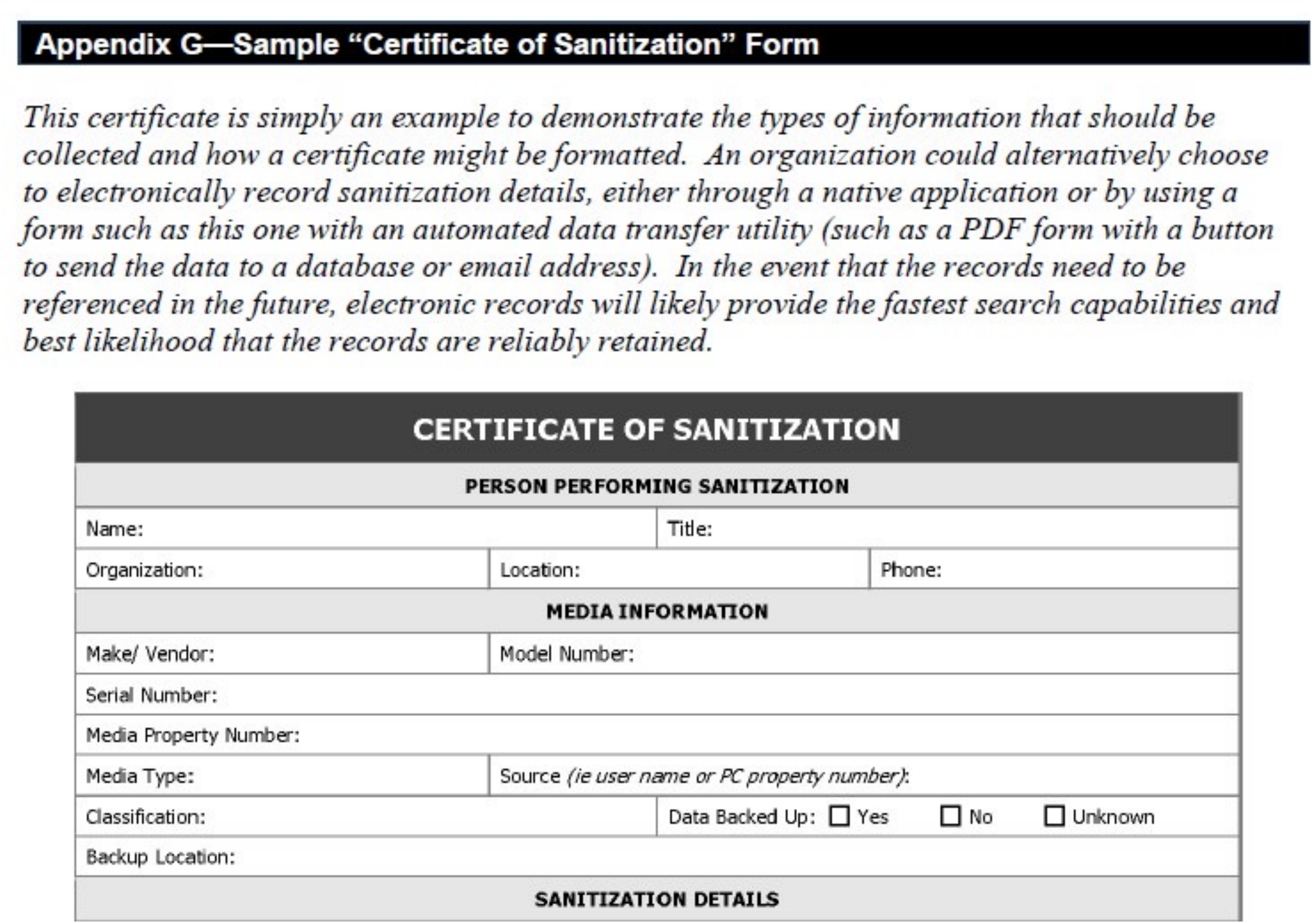
3.7.3: Ensure equipment removed for off-site maintenance is sanitized of any CUI

- ***Discussion:*** *This requirement addresses the information security aspects of system maintenance that are performed off-site and applies to all types of maintenance to any system component (including applications) conducted by a local or nonlocal entity (e.g., in-contract, warranty, in- house, software maintenance agreement).*
- *[SP 800-88] provides guidance on media sanitization.*



Flash Memory-Based Storage Devices	
ATA Solid State Drives (SSDs) *This includes PATA, SATA, eSATA, etc.*	
Clear:	1. Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used. Note: It is important to note that overwrite on flash-based media may significantly reduce the effective lifetime of the media and it may not sanitize the data in unmapped physical media (i.e., the old data may still remain on the media). 2. Use the ATA Security feature set's SECURITY ERASE UNIT command, if supported.
Purge:	Three options are available: 1. Apply the ATA sanitize command, if supported. One or both of the following options may be available: a. The block erase command. *Optionally:* After the block erase command is successfully applied to a device, write binary 1s across the user addressable area of the storage media and then perform a second block erase. b. If the device supports encryption, the Cryptographic Erase (also known as sanitize crypto scramble) command. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, Secure Erase or the Clear procedure could alternatively be applied. 2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, Secure Erase or the Clear procedure could alternatively be applied.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification must be performed for each technique within Clear and Purge as described in the Verify Methods subsection. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase.

Certificate of Sanitization Sample



Appendix G—Sample "Certificate of Sanitization" Form

This certificate is simply an example to demonstrate the types of information that should be collected and how a certificate might be formatted. An organization could alternatively choose to electronically record sanitization details, either through a native application or by using a form such as this one with an automated data transfer utility (such as a PDF form with a button to send the data to a database or email address). In the event that the records need to be referenced in the future, electronic records will likely provide the fastest search capabilities and best likelihood that the records are reliably retained.

CERTIFICATE OF SANITIZATION		
PERSON PERFORMING SANITIZATION		
Name:	Title:	
Organization:	Location:	Phone:
MEDIA INFORMATION		
Make/ Vendor:	Model Number:	
Serial Number:		
Media Property Number:		
Media Type:	Source *(ie user name or PC property number)*:	
Classification:	Data Backed Up: □ Yes □ No □ Unknown	
Backup Location:		
SANITIZATION DETAILS		

3.8.3: Sanitize or destroy system media containing CUI before disposal or release for reuse

- *Determine if:*
  - *[a] system media containing CUI is sanitized or destroyed before disposal*
  - *[b] system media containing CUI is sanitized before it is released for reuse*

3.8.3: Sanitize or destroy system media containing CUI before disposal or release for reuse

- ***<u>Discussion:</u>*** *This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal.*
- *Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization. Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for controlled unclassified information.*
- *[SP 800-88] provides guidance on media sanitization.*

3.8.3: Sanitize or destroy system media containing CUI before disposal or release for reuse

- ***Discussion:*** *This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal.*
- *Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization. Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for controlled unclassified information.*
- *[SP 800-88] provides guidance on media sanitization.*

3.8.3: Sanitize or destroy system media containing CUI before disposal or release for reuse

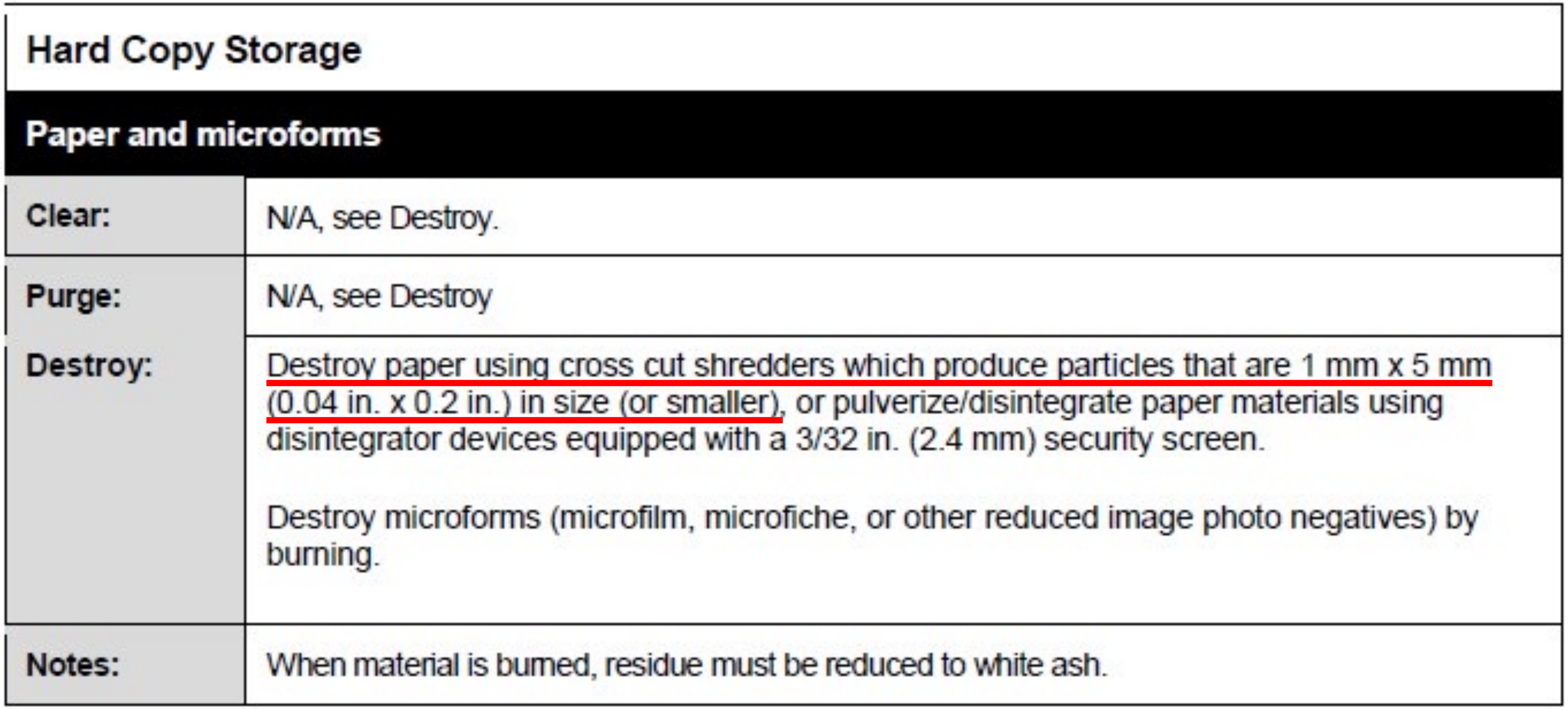
- ***Discussion:*** *This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal.*
- *Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization. Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for controlled unclassified information.*
- *[SP 800-88] provides guidance on media sanitization.*

3.8.3: Sanitize or destroy system media containing CUI before disposal or release for reuse

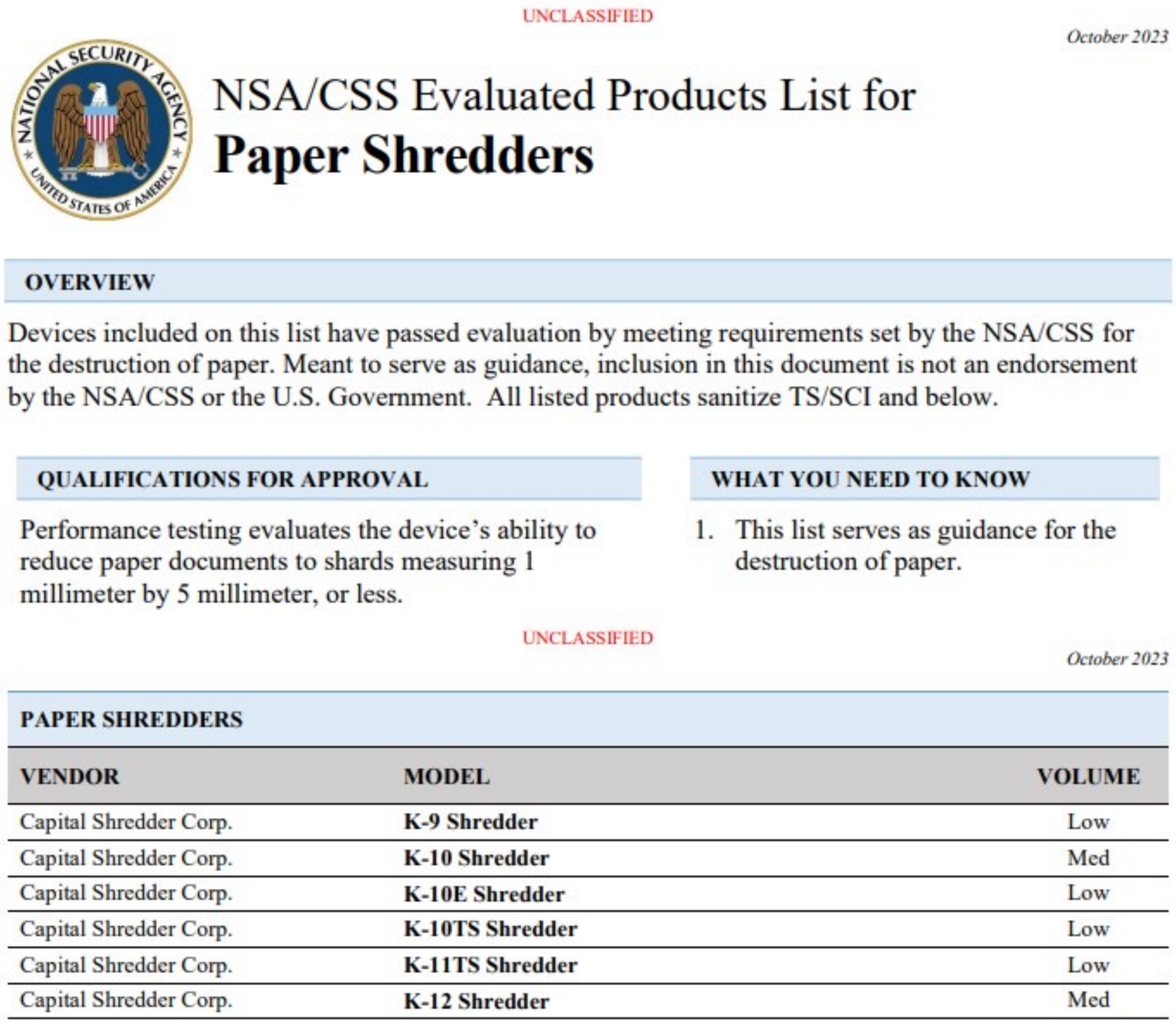
- ***Discussion:*** *This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal.*
- *Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization. Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for controlled unclassified information.*
- *[SP 800-88] provides guidance on media sanitization.*

3.8.3: Sanitize or destroy system media containing CUI before disposal or release for reuse

- ***Discussion:*** *This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal.*
- *Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization. Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for controlled unclassified information.*
- *[SP 800-88] provides guidance on media sanitization.*



Hard Copy Storage	
Paper and microforms	
Clear:	N/A, see Destroy.
Purge:	N/A, see Destroy
Destroy:	Destroy paper using cross cut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller), or pulverize/disintegrate paper materials using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen. Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning.
Notes:	When material is bumed, residue must be reduced to white ash.



UNCLASSIFIED

October 2023

NSA/CSS Evaluated Products List for **Paper Shredders**

OVERVIEW

Devices included on this list have passed evaluation by meeting requirements set by the NSA/CSS for the destruction of paper. Meant to serve as guidance, inclusion in this document is not an endorsement by the NSA/CSS or the U.S. Government. All listed products sanitize TS/SCI and below.

QUALIFICATIONS FOR APPROVAL

Performance testing evaluates the device's ability to reduce paper documents to shards measuring 1 millimeter by 5 millimeter, or less.

WHAT YOU NEED TO KNOW

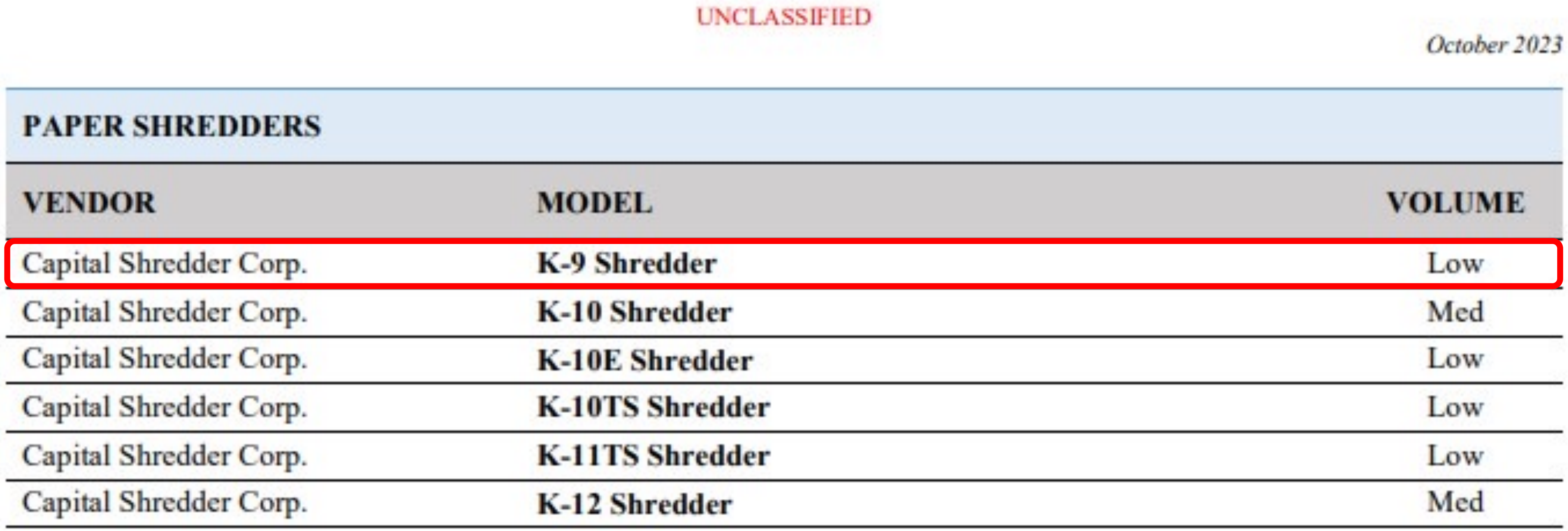
1. This list serves as guidance for the destruction of paper.

UNCLASSIFIED

October 2023

PAPER SHREDDERS

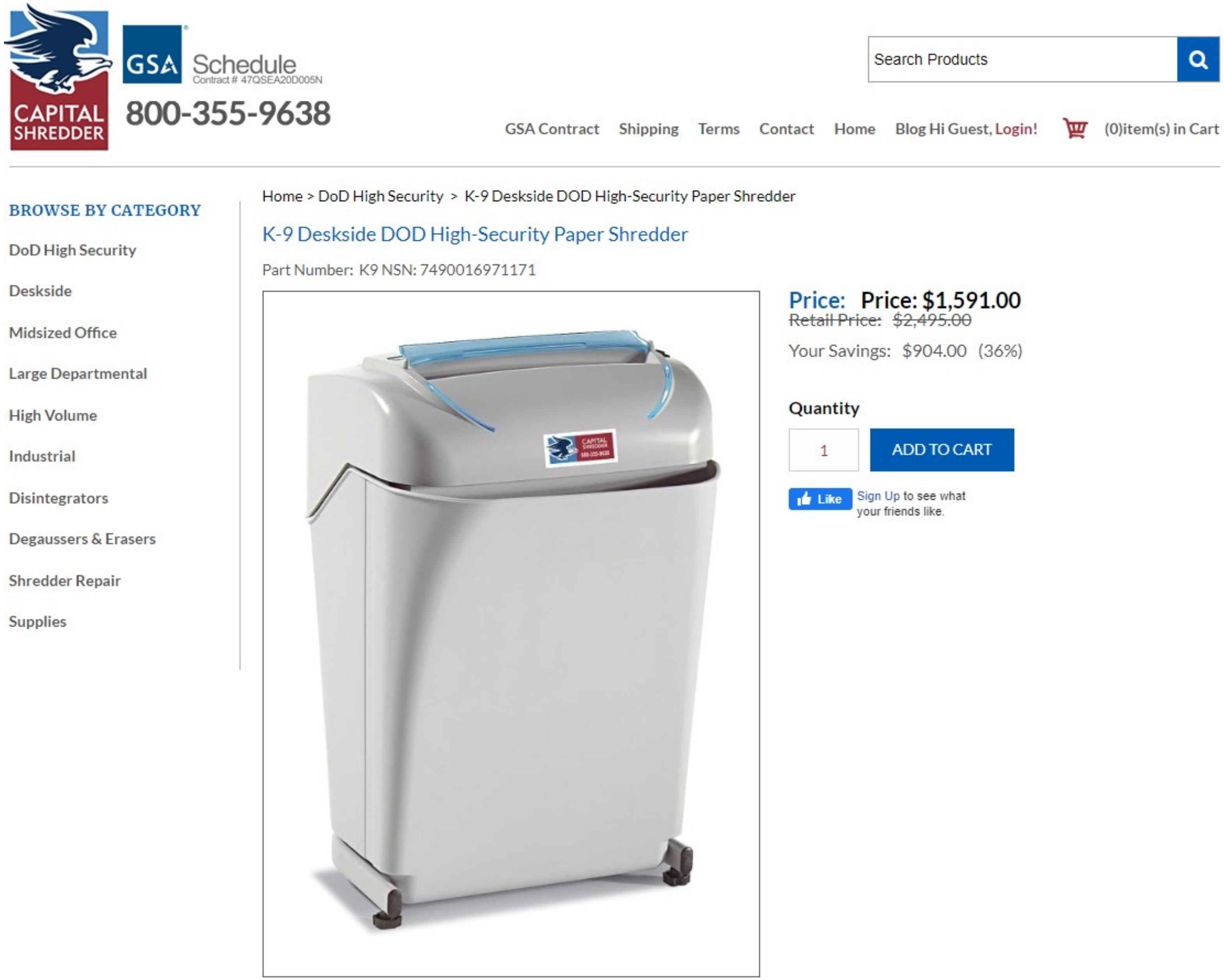
VENDOR	MODEL	VOLUME
Capital Shredder Corp.	**K-9 Shredder**	Low
Capital Shredder Corp.	**K-10 Shredder**	Med
Capital Shredder Corp.	**K-10E Shredder**	Low
Capital Shredder Corp.	**K-10TS Shredder**	Low
Capital Shredder Corp.	**K-11TS Shredder**	Low
Capital Shredder Corp.	**K-12 Shredder**	Med



UNCLASSIFIED

October 2023

PAPER SHREDDERS		
VENDOR	**MODEL**	**VOLUME**
Capital Shredder Corp.	**K-9 Shredder**	Low
Capital Shredder Corp.	**K-10 Shredder**	Med
Capital Shredder Corp.	**K-10E Shredder**	Low
Capital Shredder Corp.	**K-10TS Shredder**	Low
Capital Shredder Corp.	**K-11TS Shredder**	Low
Capital Shredder Corp.	**K-12 Shredder**	Med



CAPITAL SHREDDER

GSA Schedule
Contract # 47QSEA20D005N

800-355-9638

Search Products

GSA Contract | Shipping | Terms | Contact | Home | Blog Hi Guest, Login! | (0)item(s) in Cart

BROWSE BY CATEGORY

- DoD High Security
- Deskside
- Midsized Office
- Large Departmental
- High Volume
- Industrial
- Disintegrators
- Degaussers & Erasers
- Shredder Repair
- Supplies

Home > DoD High Security > K-9 Deskside DOD High-Security Paper Shredder

K-9 Deskside DOD High-Security Paper Shredder

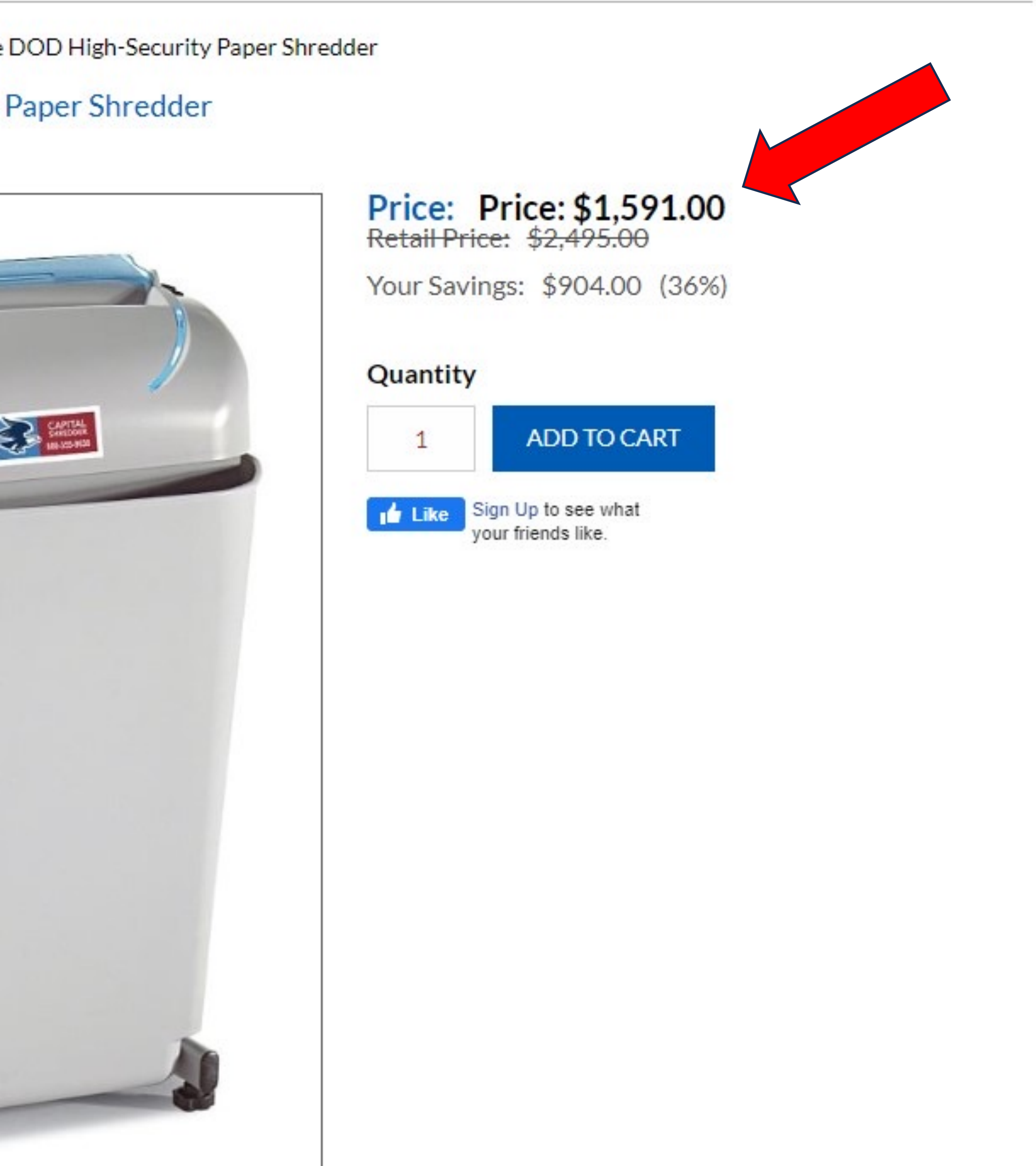
Part Number: K9 NSN: 7490016971171

Price: Price: $1,591.00
~~Retail Price: $2,495.00~~
Your Savings: $904.00 (36%)

Quantity

1 | ADD TO CART

Like | Sign Up to see what your friends like.



e DOD High-Security Paper Shredder

Paper Shredder

Price: Price: $1,591.00

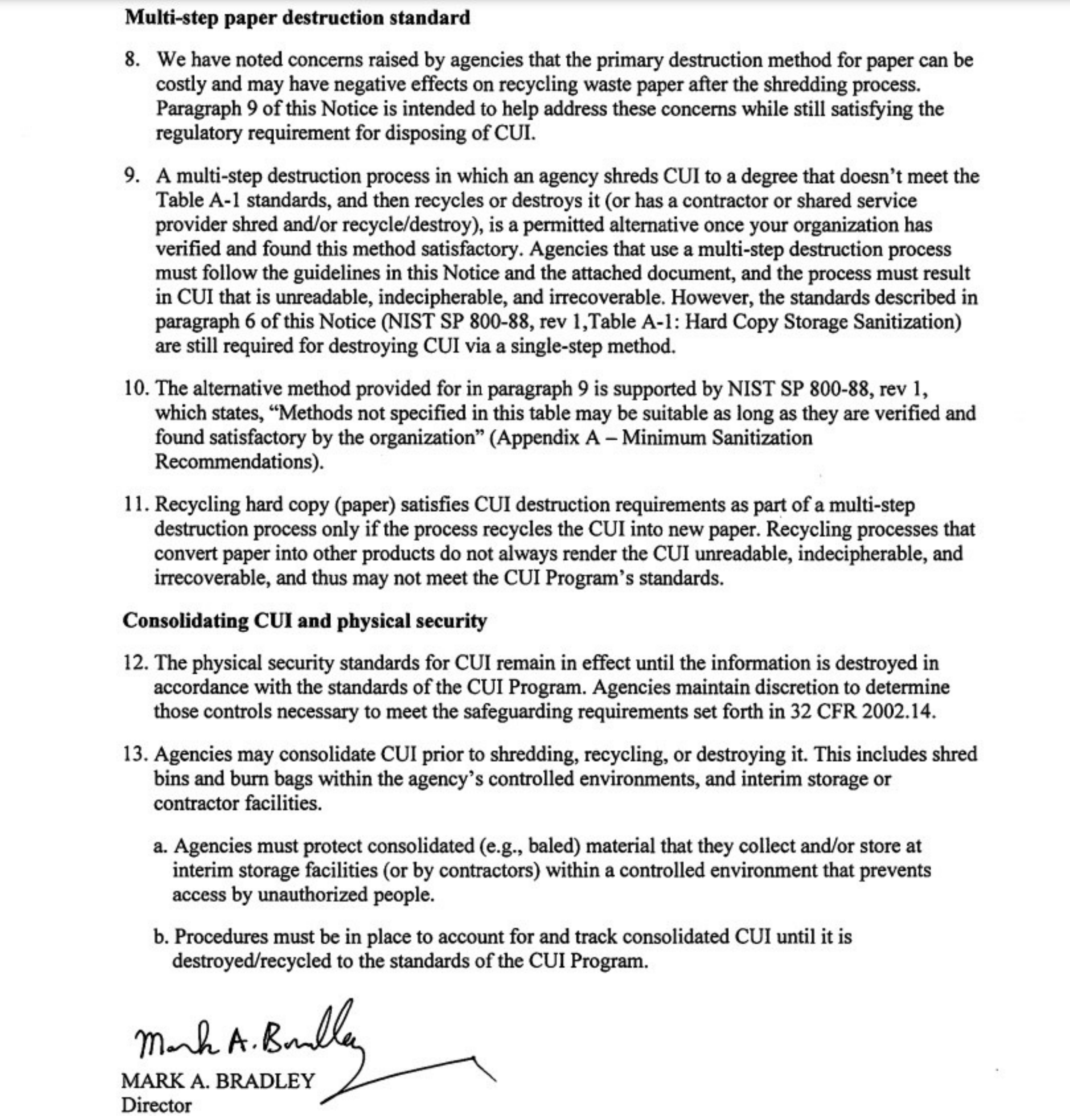
~~Retail Price: $2,495.00~~

Your Savings: $904.00 (36%)

Quantity

1

Sign Up to see what your friends like.



Multi-step paper destruction standard

8. We have noted concerns raised by agencies that the primary destruction method for paper can be costly and may have negative effects on recycling waste paper after the shredding process. Paragraph 9 of this Notice is intended to help address these concerns while still satisfying the regulatory requirement for disposing of CUI.

9. A multi-step destruction process in which an agency shreds CUI to a degree that doesn't meet the Table A-1 standards, and then recycles or destroys it (or has a contractor or shared service provider shred and/or recycle/destroy), is a permitted alternative once your organization has verified and found this method satisfactory. Agencies that use a multi-step destruction process must follow the guidelines in this Notice and the attached document, and the process must result in CUI that is unreadable, indecipherable, and irrecoverable. However, the standards described in paragraph 6 of this Notice (NIST SP 800-88, rev 1,Table A-1: Hard Copy Storage Sanitization) are still required for destroying CUI via a single-step method.

10. The alternative method provided for in paragraph 9 is supported by NIST SP 800-88, rev 1, which states, "Methods not specified in this table may be suitable as long as they are verified and found satisfactory by the organization" (Appendix A – Minimum Sanitization Recommendations).

11. Recycling hard copy (paper) satisfies CUI destruction requirements as part of a multi-step destruction process only if the process recycles the CUI into new paper. Recycling processes that convert paper into other products do not always render the CUI unreadable, indecipherable, and irrecoverable, and thus may not meet the CUI Program's standards.

Consolidating CUI and physical security

12. The physical security standards for CUI remain in effect until the information is destroyed in accordance with the standards of the CUI Program. Agencies maintain discretion to determine those controls necessary to meet the safeguarding requirements set forth in 32 CFR 2002.14.

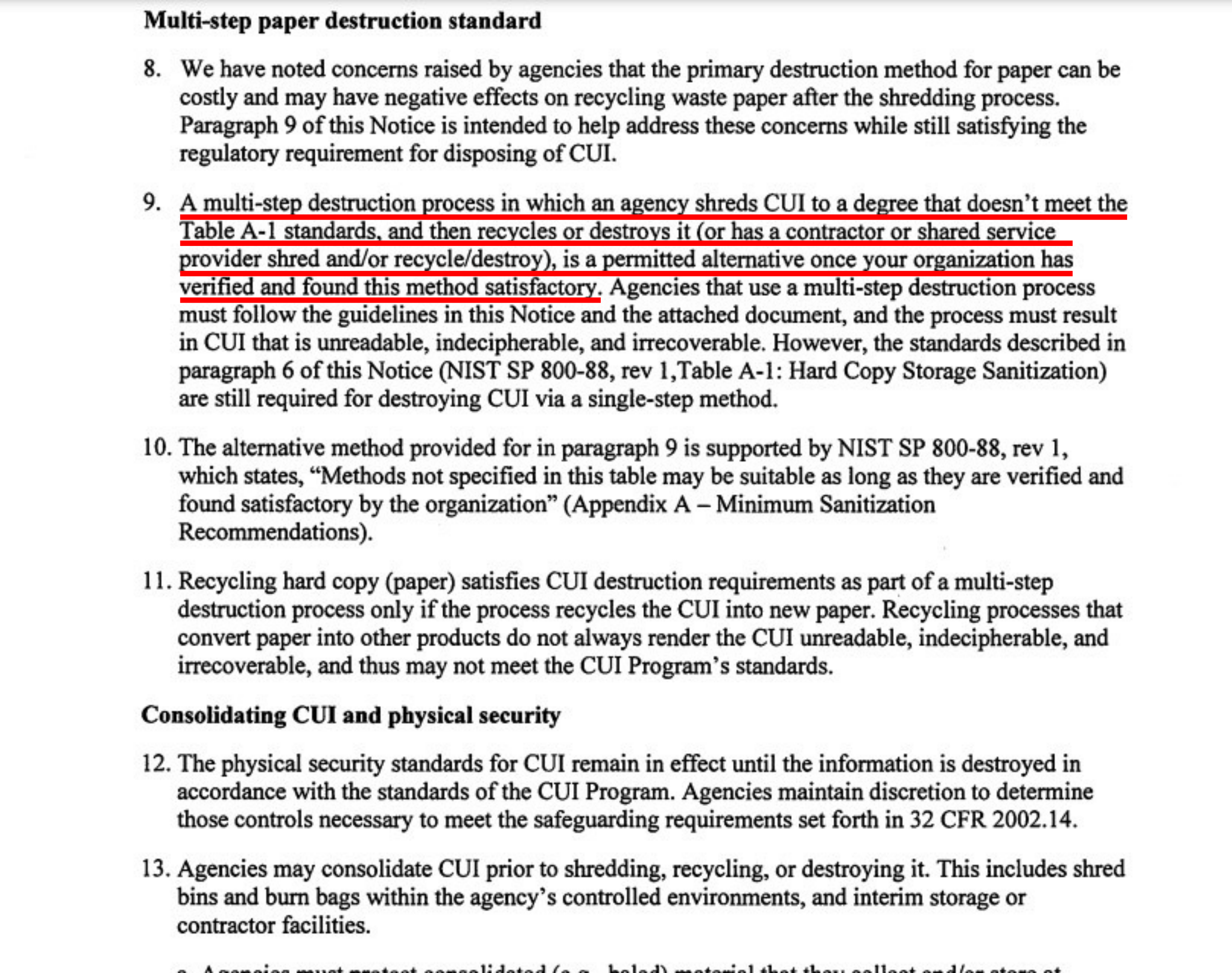
13. Agencies may consolidate CUI prior to shredding, recycling, or destroying it. This includes shred bins and burn bags within the agency's controlled environments, and interim storage or contractor facilities.

    a. Agencies must protect consolidated (e.g., baled) material that they collect and/or store at interim storage facilities (or by contractors) within a controlled environment that prevents access by unauthorized people.

    b. Procedures must be in place to account for and track consolidated CUI until it is destroyed/recycled to the standards of the CUI Program.

Mark A. Bradley

MARK A. BRADLEY
Director



Multi-step paper destruction standard

8. We have noted concerns raised by agencies that the primary destruction method for paper can be costly and may have negative effects on recycling waste paper after the shredding process. Paragraph 9 of this Notice is intended to help address these concerns while still satisfying the regulatory requirement for disposing of CUI.

9. A multi-step destruction process in which an agency shreds CUI to a degree that doesn't meet the Table A-1 standards, and then recycles or destroys it (or has a contractor or shared service provider shred and/or recycle/destroy), is a permitted alternative once your organization has verified and found this method satisfactory. Agencies that use a multi-step destruction process must follow the guidelines in this Notice and the attached document, and the process must result in CUI that is unreadable, indecipherable, and irrecoverable. However, the standards described in paragraph 6 of this Notice (NIST SP 800-88, rev 1,Table A-1: Hard Copy Storage Sanitization) are still required for destroying CUI via a single-step method.

10. The alternative method provided for in paragraph 9 is supported by NIST SP 800-88, rev 1, which states, "Methods not specified in this table may be suitable as long as they are verified and found satisfactory by the organization" (Appendix A – Minimum Sanitization Recommendations).

11. Recycling hard copy (paper) satisfies CUI destruction requirements as part of a multi-step destruction process only if the process recycles the CUI into new paper. Recycling processes that convert paper into other products do not always render the CUI unreadable, indecipherable, and irrecoverable, and thus may not meet the CUI Program's standards.

Consolidating CUI and physical security

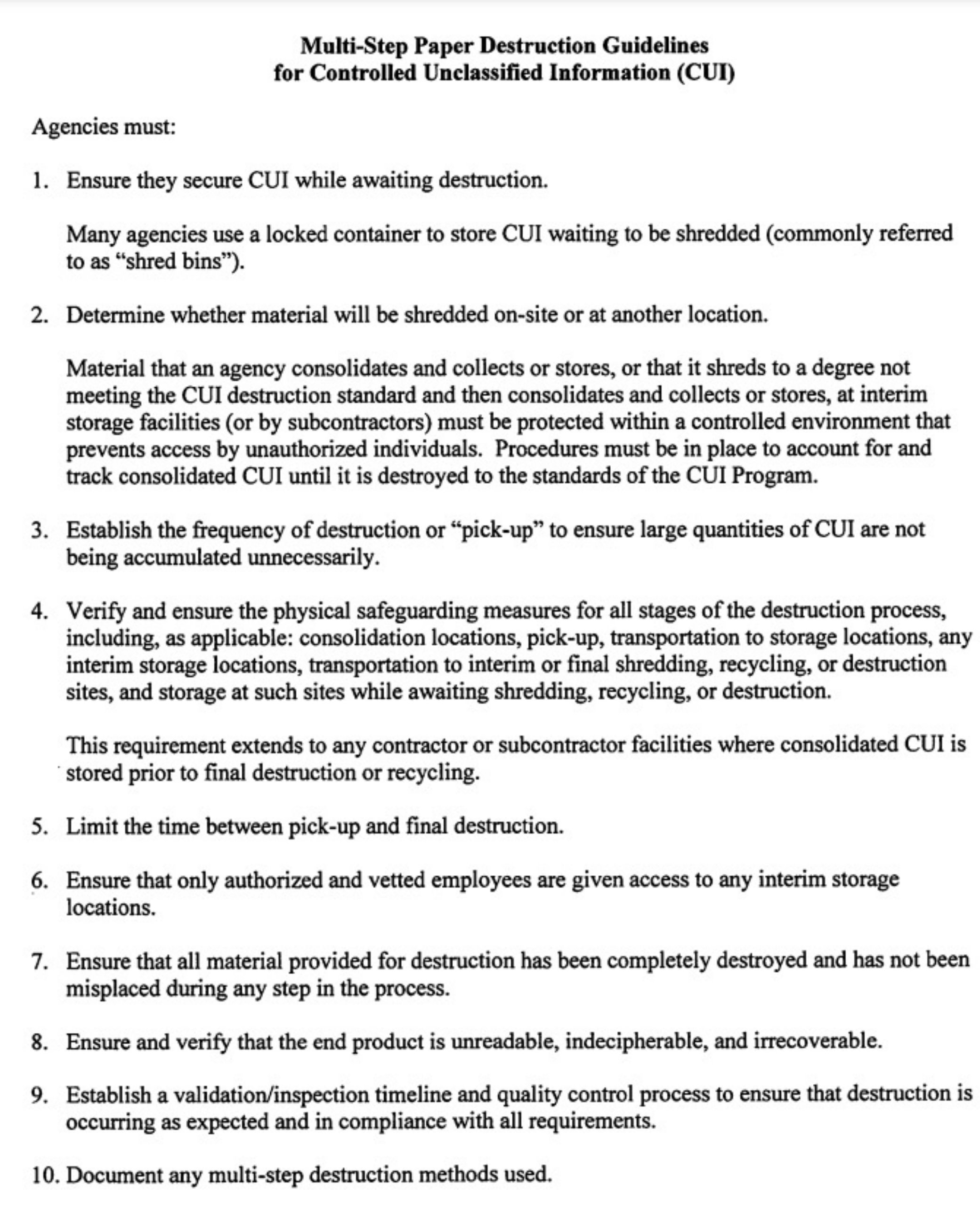
12. The physical security standards for CUI remain in effect until the information is destroyed in accordance with the standards of the CUI Program. Agencies maintain discretion to determine those controls necessary to meet the safeguarding requirements set forth in 32 CFR 2002.14.

13. Agencies may consolidate CUI prior to shredding, recycling, or destroying it. This includes shred bins and burn bags within the agency's controlled environments, and interim storage or contractor facilities.

    a. Agencies must protect consolidated (e.g., baled) material that they collect and/or store at

Potential Solution for Multistep Destruction

➕



Multi-Step Paper Destruction Guidelines for Controlled Unclassified Information (CUI)

Agencies must:

1. Ensure they secure CUI while awaiting destruction.

   Many agencies use a locked container to store CUI waiting to be shredded (commonly referred to as "shred bins").

2. Determine whether material will be shredded on-site or at another location.

   Material that an agency consolidates and collects or stores, or that it shreds to a degree not meeting the CUI destruction standard and then consolidates and collects or stores, at interim storage facilities (or by subcontractors) must be protected within a controlled environment that prevents access by unauthorized individuals. Procedures must be in place to account for and track consolidated CUI until it is destroyed to the standards of the CUI Program.

3. Establish the frequency of destruction or "pick-up" to ensure large quantities of CUI are not being accumulated unnecessarily.

4. Verify and ensure the physical safeguarding measures for all stages of the destruction process, including, as applicable: consolidation locations, pick-up, transportation to storage locations, any interim storage locations, transportation to interim or final shredding, recycling, or destruction sites, and storage at such sites while awaiting shredding, recycling, or destruction.

   This requirement extends to any contractor or subcontractor facilities where consolidated CUI is stored prior to final destruction or recycling.

5. Limit the time between pick-up and final destruction.

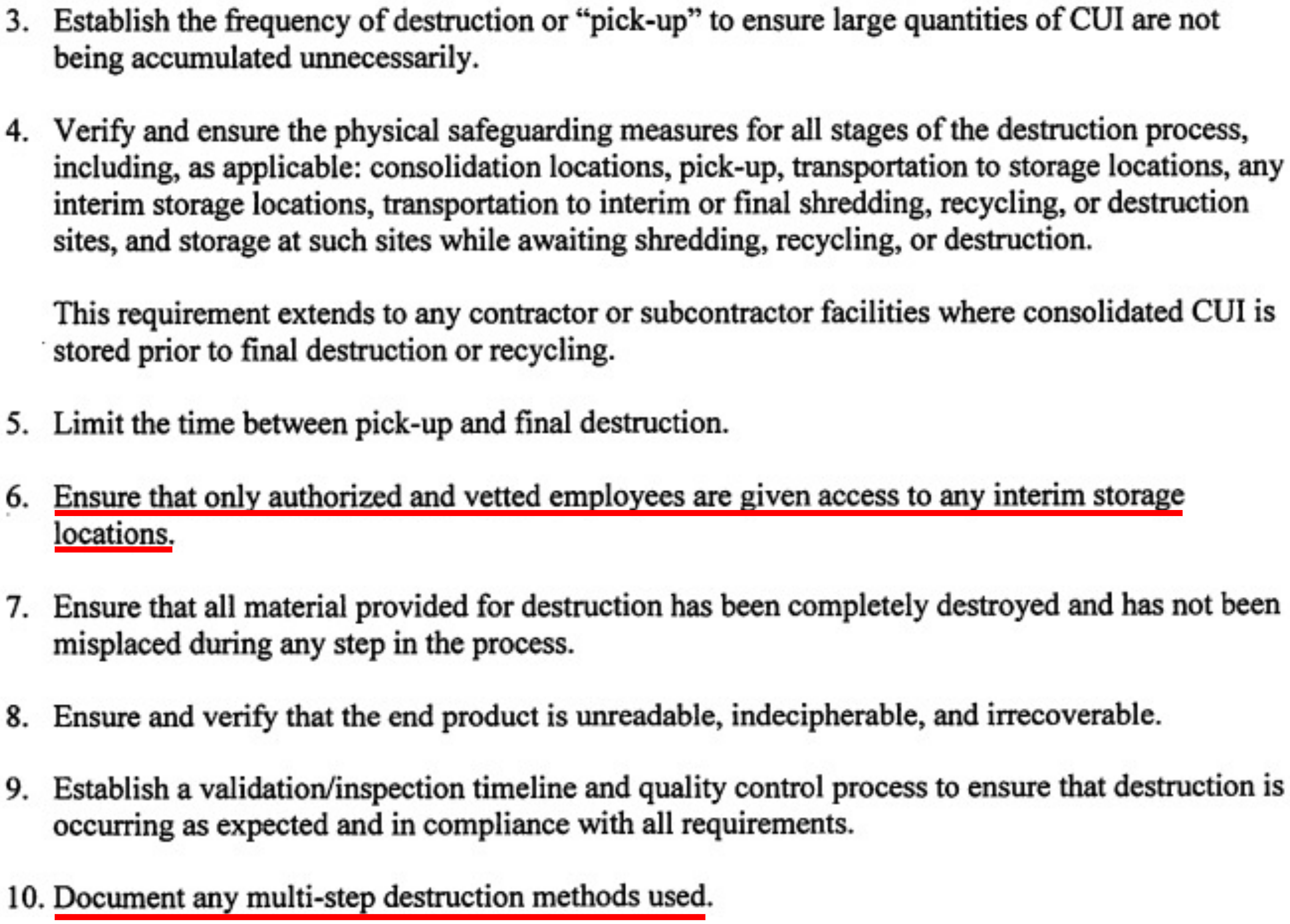
6. Ensure that only authorized and vetted employees are given access to any interim storage locations.

7. Ensure that all material provided for destruction has been completely destroyed and has not been misplaced during any step in the process.

8. Ensure and verify that the end product is unreadable, indecipherable, and irrecoverable.

9. Establish a validation/inspection timeline and quality control process to ensure that destruction is occurring as expected and in compliance with all requirements.

10. Document any multi-step destruction methods used.



3. Establish the frequency of destruction or "pick-up" to ensure large quantities of CUI are not being accumulated unnecessarily.

4. Verify and ensure the physical safeguarding measures for all stages of the destruction process, including, as applicable: consolidation locations, pick-up, transportation to storage locations, any interim storage locations, transportation to interim or final shredding, recycling, or destruction sites, and storage at such sites while awaiting shredding, recycling, or destruction.

   This requirement extends to any contractor or subcontractor facilities where consolidated CUI is stored prior to final destruction or recycling.

5. Limit the time between pick-up and final destruction.

6. Ensure that only authorized and vetted employees are given access to any interim storage locations.

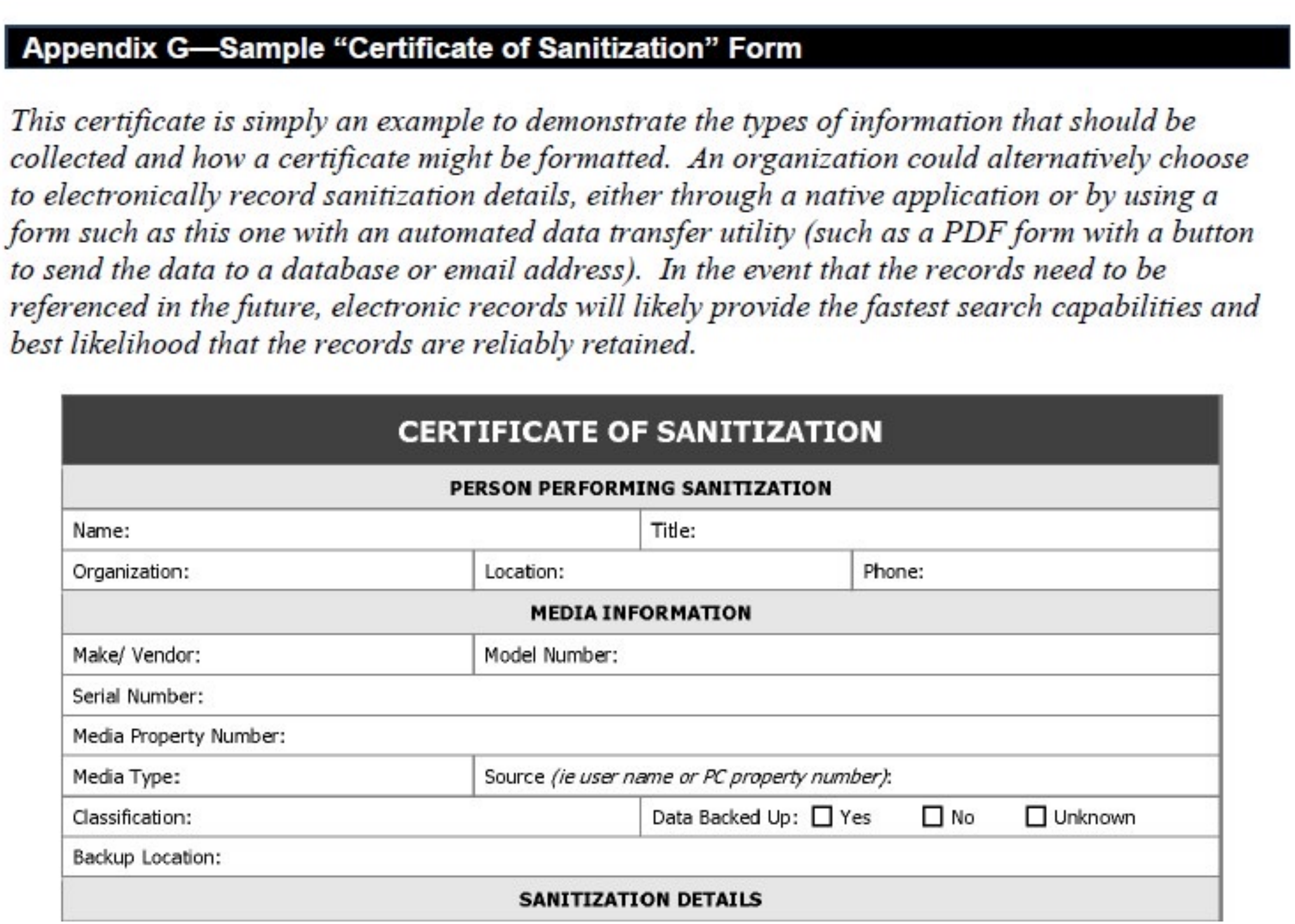
7. Ensure that all material provided for destruction has been completely destroyed and has not been misplaced during any step in the process.

8. Ensure and verify that the end product is unreadable, indecipherable, and irrecoverable.

9. Establish a validation/inspection timeline and quality control process to ensure that destruction is occurring as expected and in compliance with all requirements.

10. Document any multi-step destruction methods used.

Certificate of Sanitization Sample



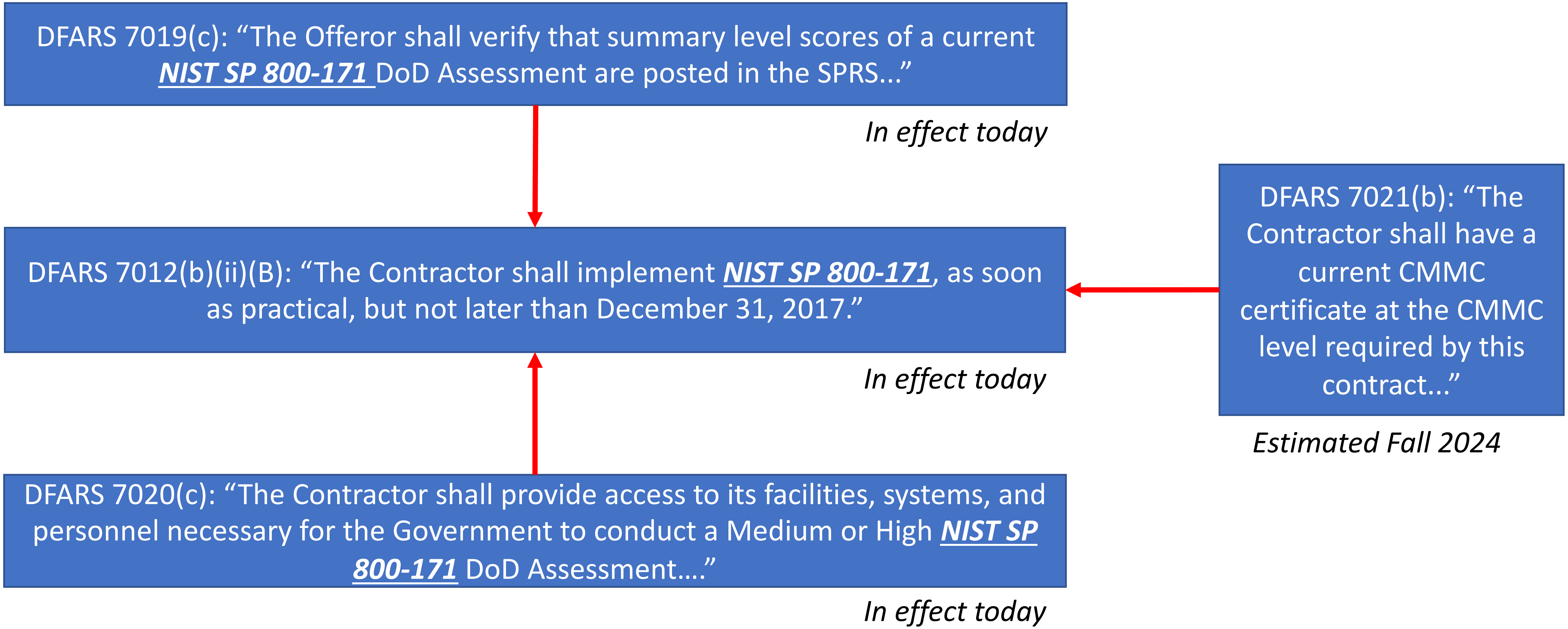
Appendix G—Sample "Certificate of Sanitization" Form

This certificate is simply an example to demonstrate the types of information that should be collected and how a certificate might be formatted. An organization could alternatively choose to electronically record sanitization details, either through a native application or by using a form such as this one with an automated data transfer utility (such as a PDF form with a button to send the data to a database or email address). In the event that the records need to be referenced in the future, electronic records will likely provide the fastest search capabilities and best likelihood that the records are reliably retained.

CERTIFICATE OF SANITIZATION

PERSON PERFORMING SANITIZATION		
Name:	Title:	
Organization:	Location:	Phone:
MEDIA INFORMATION		
Make/ Vendor:	Model Number:	
Serial Number:		
Media Property Number:		
Media Type:	Source *(ie user name or PC property number)*:	
Classification:	Data Backed Up: □ Yes □ No □ Unknown	
Backup Location:		
SANITIZATION DETAILS		

CMMC assesses ***EXISTING*** requirements in DFARS 7012



DFARS 7019(c): “The Offeror shall verify that summary level scores of a current ***NIST SP 800-171*** DoD Assessment are posted in the SPRS...”

In effect today

DFARS 7012(b)(ii)(B): “The Contractor shall implement ***NIST SP 800-171***, as soon as practical, but not later than December 31, 2017.”

In effect today

DFARS 7021(b): “The Contractor shall have a current CMMC certificate at the CMMC level required by this contract...”

Estimated Fall 2024

DFARS 7020(c): “The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High ***NIST SP 800-171*** DoD Assessment....”

In effect today

References

- DFARS Definition: https://www.federalregister.gov/defense-federal-acquisition-regulation-supplement-dfars-
- DFARS 252.204-7012: https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.
- DFARS 252.204-7019: https://www.acquisition.gov/dfars/252.204-7019-notice-nistsp-800-171-dod-assessment-requirements.
- DFARS 252.204-7020: https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements.
- DFARS 252.204-7021: https://www.acquisition.gov/dfars/252.204-7021-cybersecurity-maturity-model-certification-requirements.
- DFARS 252.204-7024: https://www.acquisition.gov/dfars/252.204-7024-notice-use-supplier-performance-risk-system.

- NIST SP 800-171 and NIST SP 800-171A: https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final
- NIST SP 800-128: https://csrc.nist.gov/pubs/sp/800/128/upd1/final
- DoD Instruction 5230.24: https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/523024p.pdf
- CUI Policy and Guidance: https://www.archives.gov/cui/registry/policy-guidance
- NSA Evaluated Products List: https://www.nsa.gov/Resources/Media-Destruction-Guidance/NSA-Evaluated-Products-Lists-EPLs/
- DoD Assessment Methodology: https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf

Questions

?

Fernando Machado
CISO, Cybersec Investments

THE CYBER AB
CMMC CERTIFICATION
AUTHORIZED C3PAO

- **Services**:
  - CMMC Advisory Services
  - CMMC Readiness Assessments
  - Joint Surveillance Voluntary Assessments (JSVA)
  - NIST SP 800-171 3rd Party Letter of Attestation

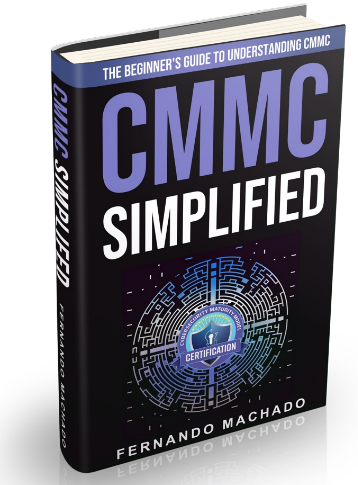
www.cybersecinvestments.com

info@cybersecinvestments.com

1-800-960-8802

CAICO
CERTIFIED CMMC ASSESSOR

amazon



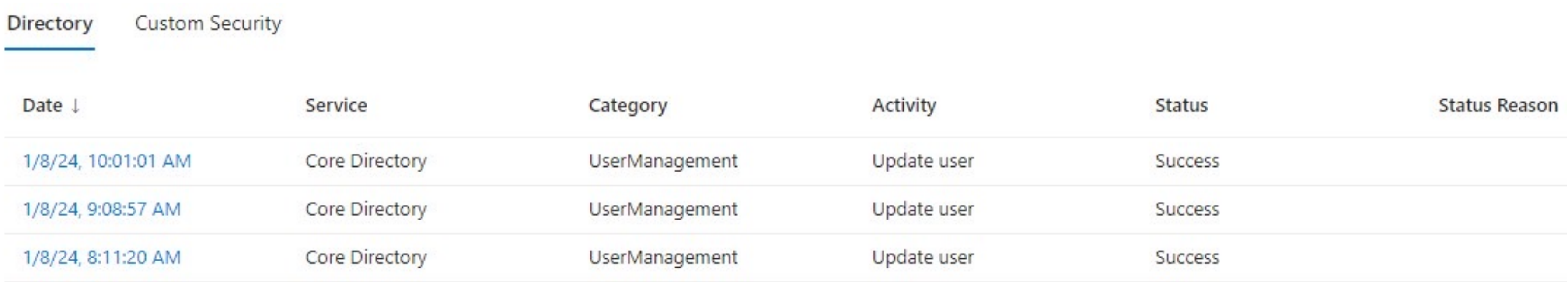
LinkedIn

CAICO
CERTIFIED CMMC PROFESSIONAL

Extra Slides

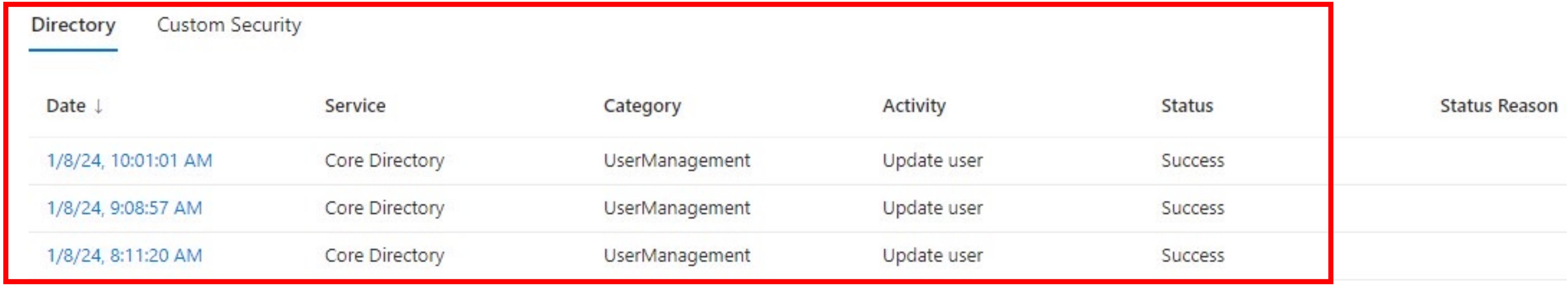
[b] *the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined*

- Examples may include: Audit logs
  - *Date (e.g., date and time of the occurrence)*
  - *Service (e.g., service that logged the occurrence)*
  - *Category (e.g., category and name of the activity (what))*
  - *Status (e.g., status of the activity (success or failure))*



Date ↓	Service	Category	Activity	Status	Status Reason
1/8/24, 10:01:01 AM	Core Directory	UserManagement	Update user	Success	
1/8/24, 9:08:57 AM	Core Directory	UserManagement	Update user	Success	
1/8/24, 8:11:20 AM	Core Directory	UserManagement	Update user	Success	

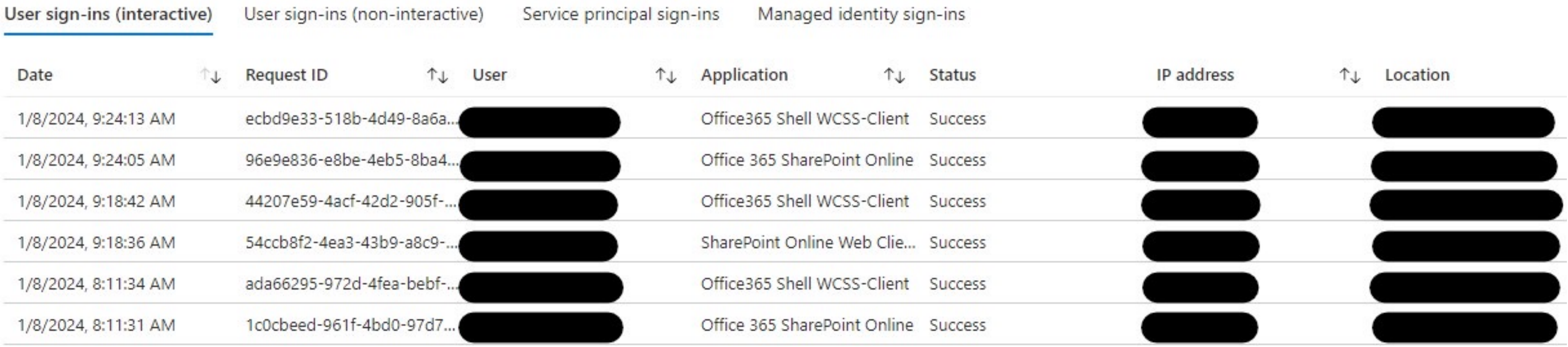
(b) the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined



Date ↓	Service	Category	Activity	Status	Status Reason
1/8/24, 10:01:01 AM	Core Directory	UserManagement	Update user	Success	
1/8/24, 9:08:57 AM	Core Directory	UserManagement	Update user	Success	
1/8/24, 8:11:20 AM	Core Directory	UserManagement	Update user	Success	

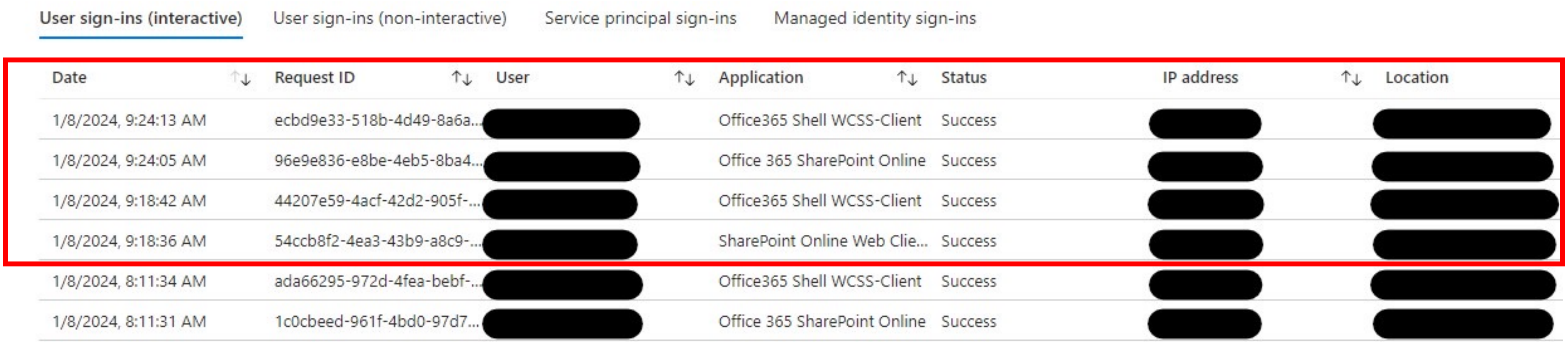
[b] *the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined*

- Examples may include: Sign-in logs
  - *Date (e.g., sign-in date)*
  - *Request ID*
  - *User (e.g., Username or User ID)*
  - *Status (e.g., status of the sign-in)*


User sign-ins (interactive)
User sign-ins (non-interactive)
Service principal sign-ins
Managed identity sign-ins

Date	Request ID	User	Application	Status	IP address	Location
1/8/2024, 9:24:13 AM	ecbd9e33-518b-4d49-8a6a...	[redacted]	Office365 Shell WCSS-Client	Success	[redacted]	[redacted]
1/8/2024, 9:24:05 AM	96e9e836-e8be-4eb5-8ba4...	[redacted]	Office 365 SharePoint Online	Success	[redacted]	[redacted]
1/8/2024, 9:18:42 AM	44207e59-4acf-42d2-905f-...	[redacted]	Office365 Shell WCSS-Client	Success	[redacted]	[redacted]
1/8/2024, 9:18:36 AM	54ccb8f2-4ea3-43b9-a8c9-...	[redacted]	SharePoint Online Web Clie...	Success	[redacted]	[redacted]
1/8/2024, 8:11:34 AM	ada66295-972d-4fea-bebf-...	[redacted]	Office365 Shell WCSS-Client	Success	[redacted]	[redacted]
1/8/2024, 8:11:31 AM	1c0cbeed-961f-4bd0-97d7...	[redacted]	Office 365 SharePoint Online	Success	[redacted]	[redacted]

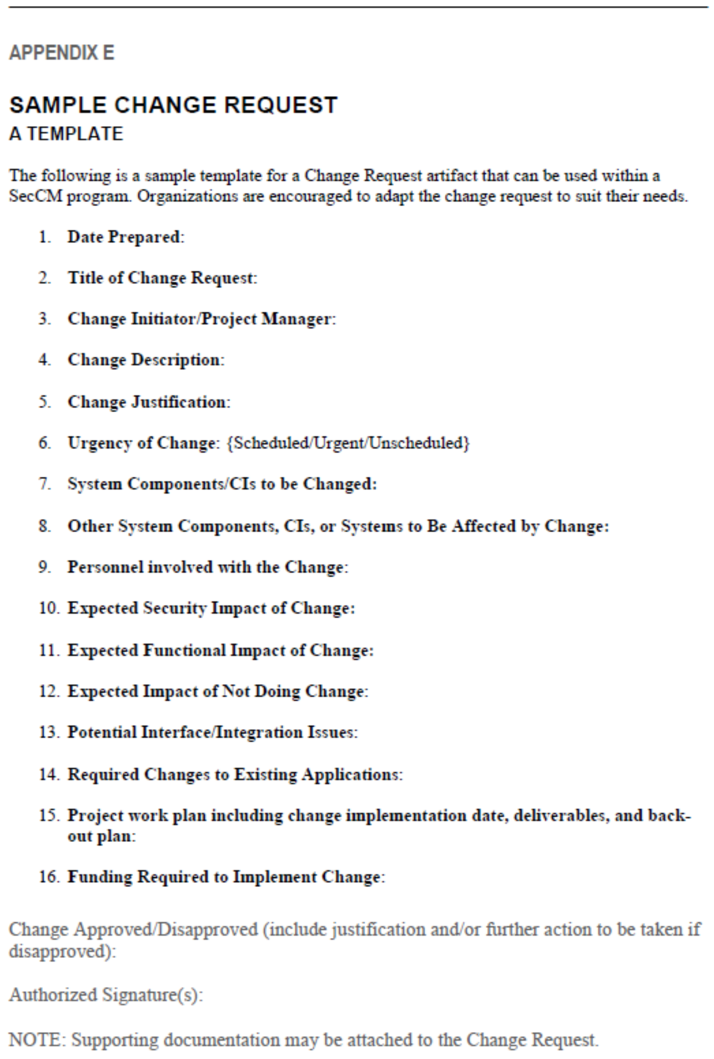
[b] the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined


User sign-ins (interactive)
User sign-ins (non-interactive)
Service principal sign-ins
Managed identity sign-ins

Date	Request ID	User	Application	Status	IP address	Location
1/8/2024, 9:24:13 AM	ecbd9e33-518b-4d49-8a6a...	[redacted]	Office365 Shell WCSS-Client	Success	[redacted]	[redacted]
1/8/2024, 9:24:05 AM	96e9e836-e8be-4eb5-8ba4...	[redacted]	Office 365 SharePoint Online	Success	[redacted]	[redacted]
1/8/2024, 9:18:42 AM	44207e59-4acf-42d2-905f-...	[redacted]	Office365 Shell WCSS-Client	Success	[redacted]	[redacted]
1/8/2024, 9:18:36 AM	54ccb8f2-4ea3-43b9-a8c9-...	[redacted]	SharePoint Online Web Clie...	Success	[redacted]	[redacted]
1/8/2024, 8:11:34 AM	ada66295-972d-4fea-bebf-...	[redacted]	Office365 Shell WCSS-Client	Success	[redacted]	[redacted]
1/8/2024, 8:11:31 AM	1c0cbeed-961f-4bd0-97d7...	[redacted]	Office 365 SharePoint Online	Success	[redacted]	[redacted]

[a] changes to the system are tracked

- *Potential solution:*
  - *Configuration Change Management*
  - *Change Request*
- *Tracking examples include:*
  - *Year/month/day/request*
    - *(e.g., 20240222-01)*
  - *Title of Change Request*



APPENDIX E

SAMPLE CHANGE REQUEST

A TEMPLATE

The following is a sample template for a Change Request artifact that can be used within a SecCM program. Organizations are encouraged to adapt the change request to suit their needs.

1. **Date Prepared**:
2. **Title of Change Request**:
3. **Change Initiator/Project Manager**:
4. **Change Description**:
5. **Change Justification**:
6. **Urgency of Change**: {Scheduled/Urgent/Unscheduled}
7. **System Components/CIs to be Changed:**
8. **Other System Components, CIs, or Systems to Be Affected by Change:**
9. **Personnel involved with the Change**:
10. **Expected Security Impact of Change:**
11. **Expected Functional Impact of Change**:
12. **Expected Impact of Not Doing Change**:
13. **Potential Interface/Integration Issues**:
14. **Required Changes to Existing Applications**:
15. **Project work plan including change implementation date, deliverables, and back-out plan**:
16. **Funding Required to Implement Change**:

Change Approved/Disapproved (include justification and/or further action to be taken if disapproved):

Authorized Signature(s):

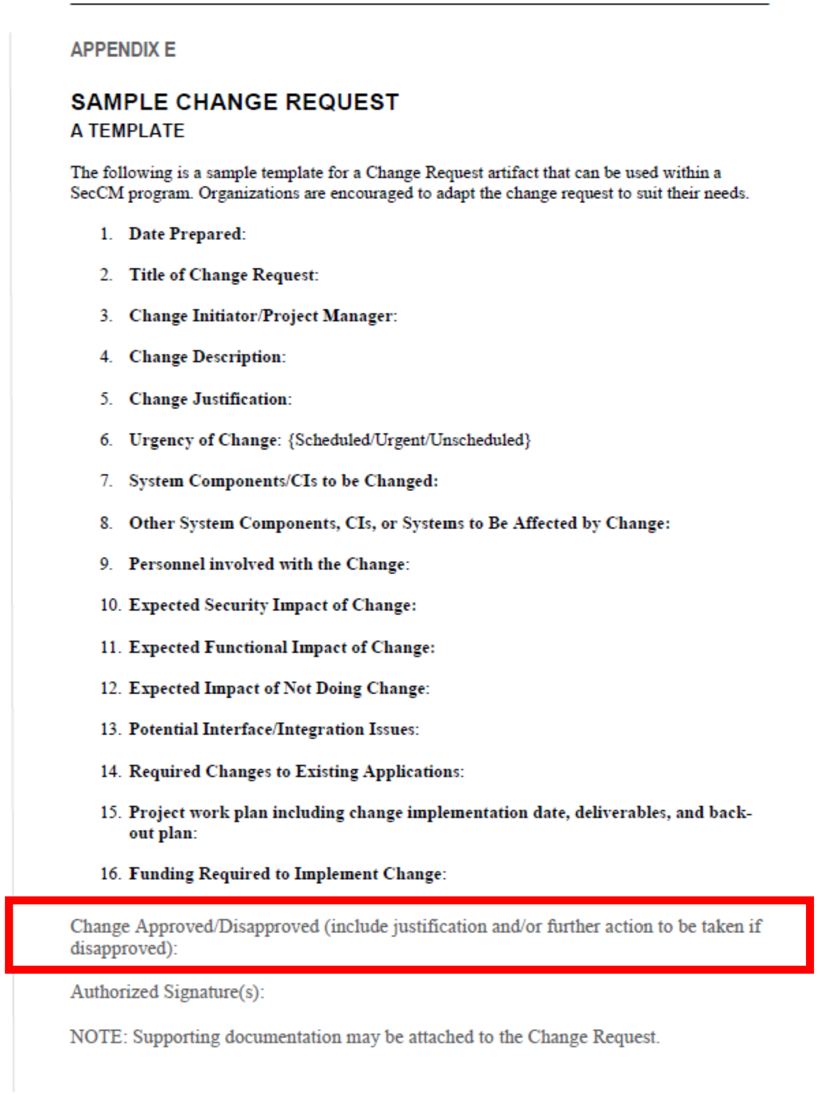
NOTE: Supporting documentation may be attached to the Change Request.

3.4.3: Track, review, approve or disapprove, and log changes to organizational systems

- *Determine if:*
  - *[a] changes to the system are tracked.*
  - *[b] changes to the system are reviewed.*
  - *[c] changes to the system are approved or disapproved.*
  - *[d] changes to the system are logged.*

[b] changes to the system are reviewed
[c] changes to the system are approved or disapproved
[d] changes to the system are logged

- *Examples of review include:*
  - Change Control Board



APPENDIX E

SAMPLE CHANGE REQUEST

A TEMPLATE

The following is a sample template for a Change Request artifact that can be used within a SecCM program. Organizations are encouraged to adapt the change request to suit their needs.

1. **Date Prepared**:
2. **Title of Change Request**:
3. **Change Initiator/Project Manager**:
4. **Change Description**:
5. **Change Justification**:
6. **Urgency of Change**: {Scheduled/Urgent/Unscheduled}
7. **System Components/CIs to be Changed:**
8. **Other System Components, CIs, or Systems to Be Affected by Change:**
9. **Personnel involved with the Change**:
10. **Expected Security Impact of Change:**
11. **Expected Functional Impact of Change:**
12. **Expected Impact of Not Doing Change**:
13. **Potential Interface/Integration Issues**:
14. **Required Changes to Existing Applications**:
15. **Project work plan including change implementation date, deliverables, and back-out plan**:
16. **Funding Required to Implement Change**:

Change Approved/Disapproved (include justification and/or further action to be taken if disapproved):

Authorized Signature(s):

NOTE: Supporting documentation may be attached to the Change Request.